

11 DE MAIO DE 2021



## Proposta Comercial

Licença de software de segurança para estações de trabalho (end points) e servidores para 48 meses;

Cliente: TRT13

Norberto Lucena  
NetSafe Corp

[norberto.lucena@netsafecorp.com.br](mailto:norberto.lucena@netsafecorp.com.br)

## Controle de Versões

### Registro

<b>Data</b>	<b>Autor</b>	<b>Versão</b>	<b>Histórico</b>
11/05/2021	Norberto Lucena	v1	Gerente de Contas

### Revisores

<b>Data</b>	<b>Revisor</b>	<b>Versão</b>	<b>Cargo</b>
11/05/2021	Eduardo Vargas	v1	Pré vendas
11/05/2021	Norberto Lucena	v1	Gerente de Contas

### Distribuição

<b>Nome</b>	<b>Cargo</b>	<b>Empresa</b>
Raimundo José Campos Jr.	Secretaria de Tecnologia da Informação e Comunicação	TRT13



## Conteúdo

---

-----	0
<b>Controle de Versões</b> -----	<b>1</b>
Registro -----	1
Revisores -----	1
Distribuição -----	1
<b>Conteúdo</b> -----	<b>2</b>
<b>1. Objetivo</b> -----	<b>3</b>
<b>2. Solução Proposta</b> -----	<b>3</b>
<b>3. Solução Proposta</b> -----	<b>3</b>
<b>4. Condições Comerciais</b> -----	<b>4</b>
6.1. Validade: -----	4
6.2. Condição de Pagamento: -----	4
6.3. -----	4
6.4. Dados Cadastrais: -----	4
<b>5. Benefício NetSafe Corp</b> -----	<b>5</b>
7.1. Suporte NetSafe Corp -----	5
<b>6. Considerações Finais</b> -----	<b>5</b>
<b>7. Termo de Aceite</b> -----	<b>6</b>
<b>8. Nossos Parceiros</b> -----	<b>7</b>

## 1. Objetivo

---

Objeto a contratação de empresa especializada para Licença de software de segurança para estações de trabalho (end points) e servidores para 48 meses;

## 2. Solução Proposta

---

Solução corporativa endpoint;

## 3. Serviços

---

Atualização de suíte para proteção de estações de trabalho e servidores.

Serviço de implementação e migração;

Treinamento/atualização tecnológica;



## 4. Condições Comerciais

Condições comerciais para Software e Serviços:

### PROPOSTA COMERCIAL

#### GRUPO ÚNICO

Item	Descrição	Unidade	Qtd.	Valor (R\$)	Valor Global (48 meses) (R\$)
1	Licença de software McAfee de segurança para estações de trabalho (endpoints) e servidores + Console de Gerenciamento Garantia Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por <b>48 meses</b> .	Nº de licenças	82.809	R\$ 224,16	R\$ 18.562.465,44
2	Licença de software McAfee de segurança para ambiente virtualizado + Console de Gerenciamento Garantia Atualizações / Suporte Técnico Manutenção Preventiva e Corretiva por <b>48 meses</b> .	Nº de licenças	5.139	R\$ 391,20	R\$ 2.010.376,80
3	Implantação e configuração da solução + Repasse de conhecimento hands-on	Serviço	28	R\$ 26.000,00	R\$ 728.000,00
4	Treinamento EAD de capacitação técnica para administração da solução	Nº de alunos	185	R\$ 3.880,00/aluno	R\$ 717.800,00
<b>Valor Global da Proposta R\$ 22.018.642,24</b>					

**Valor Total por Extenso R\$ 22.018.642,24 (Vinte e dois milhões dezoito mil seiscentos e quarenta e dois reais e vinte e quatro centavos).**



- Os preços constantes nesta proposta são válidos única e exclusivamente para a contratação em sua totalidade, Valor prestação do serviço, com todos os impostos inclusos e destacados;



4.1 **Validade:** 30 (trinta) dias;

4.2 **Condição de Pagamento:** (30) dias a partir do aceite técnico na Nota Fiscal;

4.3 **Dados Cadastrais:**

Nome da empresa: NETSAFE CORP
CNPJ: 03.476.184/0002-30
Endereço: Avenida Antonio de Goes nº60 Edf JCMP 14º sala 1433
Telefone: (81) 81 99608-7776
Responsável pela proposta: Norberto Lucena
CPF do responsável pela proposta: 043.095.654-17 SSP/PE

## 5. Benefício Exclusivo

---

### Suporte NetSafe Corp

A NetSafe se destaca no mercado por seu atendimento diferenciado, pois conta com técnicos certificados e altamente qualificados, o que garante a assertividade do nosso serviço de suporte técnico. Além disso a NetSafe é fiscalizada e auditada em sua qualidade e eficiência pelos nossos parceiros o que garante ao cliente um melhor atendimento.

Para fortalecer a parceria junto aos nossos clientes, oferecemos serviço de suporte técnico na modalidade 8x5 em 1º e 2º nível, à todos os clientes que adquirem nossas soluções, sem a cobrança de taxa adicional.

Este suporte é valido pela vigência do contrato da solução adquirida pelo cliente.

No caso onde seja necessário escalar o chamado ao fabricante, o SLA valido passará a ser o do fabricante do produto em questão.

## 6. Considerações Finais

---

Esperamos que as informações contidas neste documento sejam de grande benefício para o TRT13Se ao final da leitura, houver qualquer dúvida ou mesmo falta de alguma informação, solicitamos entrar em contato direto com o time indicado abaixo, que foi responsável pela elaboração desta proposta.

Nome	Função	Contatos
<b>Norberto Lucena</b>	Gerente de Contas	T.: 55 81 9.9608-7776 M: <a href="mailto:norberto.lucena@netsafecorp.com.br">norberto.lucena@netsafecorp.com.br</a>
<b>Eduardo Vargas</b>	Arquiteta de Soluções	M: <a href="mailto:eduardo.vargas@netsafecorp.com.br">eduardo.vargas@netsafecorp.com.br</a>

A handwritten signature in blue ink, appearing to be "JL", is located in the bottom right corner of the page.

## 7. Termo de Aceite

---

Declaro aceitar todos os termos e condições constantes nesta proposta comercial, e mediante a assinatura deste Termo de Aceite, a **NetSafe Corp** poderá processar a ordem de compra, emitir respectiva fatura e realizar a entrega dos produtos, com o nosso compromisso de efetuar o pagamento correspondente.

Endereço de faturamento:

\_\_\_\_\_

CNPJ: \_\_\_\_\_ Inscr. Estadual: \_\_\_\_\_

Inscr. Municipal: \_\_\_\_\_

Endereço para entrega: \_\_\_\_\_

\_\_\_\_\_

Brasília-DF, \_\_\_\_ de \_\_\_\_\_ de \_\_\_\_\_.

Nome Responsável (cliente): \_\_\_\_\_

Cargo: \_\_\_\_\_

Assinatura: \_\_\_\_\_

➤ Será emitido Pedido de Compra e/ou Contrato por parte do cliente? ( ) sim ( ) não

**Comentários Adicionais:**

## 8. Nossos Parceiros

---





ABOUTNET INFORMATICA LTDA - EPP  
C.N.P.J.: 07.751.724/0001-16  
I.E. 799.118.325.112  
Fone/Fax: 11 5612 8200

São Bernardo do Campo, 11/05/2021

**Ao**  
**Tribunal Regional do Trabalho 13ª Região - Paraíba**  
**Att.: Marcos Vinicius Beton Amorim**  
**Email: [rjcampos@trt13.jus.br](mailto:rjcampos@trt13.jus.br)**

Prezado Senhor, conforme solicitado, segue abaixo, nossa proposta comercial referente à ao fabricante McAfee.

### III. PLANILHA DE ESTIMATIVAS – LOTE ÚNICO

	Qt.	Valor Unitário	Valor Total
ITEM 1	82.809	R\$ 235,36	R\$ 19.489.926,24
ITEM 2	5.139	R\$ 402,73	R\$ 2.069.629,47
IMPLEMENTACAO	28	R\$ 27.300,00	R\$ 764.400,00
TREINAMENTO	185	R\$ 4.112,80	R\$ 760.868,00
		<b>Total</b>	<b>R\$ 23.084.823,71</b>

### IV. ESPECIFICAÇÃO TÉCNICA

A solução de software de segurança e os serviços oferecidos devem atender aos seguintes requisitos técnicos:

#### 1. Requisitos Gerais – Comuns aos itens 1 e 2

- 1.1. O console de gerenciamento deve estar disponível para instalação On-Premise ou utilização em nuvem (cloud do fabricante). Na opção On-Premise pode ser fornecido como um appliance virtual ou executável para instalação em servidores Windows que contemple o console SaaS /Cloud que faz parte do licenciamento.
  - 1.1.1. Para o caso de appliance virtual, deverá suportar no mínimo o Hypervisor VMWare vSphere 6.7 ou superior;
  - 1.1.2. Para o caso de instalação em sistema operacional Windows, deverá ser compatível, no mínimo, com a versão Microsoft Windows Server 2016 ou superior.
- 1.2. A solução deve possuir console de gerenciamento centralizado com acesso via WEB (HTTPS) ou MMC (Microsoft Management Console);
- 1.3. O console de gerenciamento deve ser único e capaz de gerenciar todos os dispositivos (endpoints e servidores);
- 1.4. O Console de Gerenciamento deve conter:
  - 1.4.1. Painel para monitoramento;
  - 1.4.2. Capacidade de criação de relatórios;
  - 1.4.3. Mecanismo para envio de notificações administrativas (e-mail);
- 1.5. Deve permitir inventário das máquinas gerenciadas pela solução
- 1.6. A console central deve mostrar quantos dispositivos estão sendo gerenciados e quais seus sistemas operacionais.

- 1.7. Todos os softwares, módulos e plugins pertencentes à solução de segurança deverão ser administrados pela mesma console de gerenciamento.
- 1.8. Deve possuir a capacidade de autenticação dos usuários da console de gerenciamento através do Microsoft Active Directory.
  - 1.8.1. Deve permitir a definição de perfis com diferentes níveis de privilégios de administração da solução, baseados em usuários ou grupos do Microsoft Active Directory.
  - 1.8.2. Capacidade de exportar relatórios para os seguintes tipos de arquivos, no mínimo: PDF, HTML e CSV.
  - 1.8.3. Capacidade de enviar e-mails para contas específicas, em caso de algum evento.
  - 1.8.4. A console de gerenciamento deve fornecer as seguintes informações dos computadores protegidos:
    - 1.8.4.1. Horário da última conexão da máquina com o servidor administrativo ou, no mínimo, o tempo decorrido desde a última conexão;
    - 1.8.4.2. Data e horário da última verificação executada na máquina;
    - 1.8.4.3. Se o antivírus está instalado;
    - 1.8.4.4. Versão do antivírus instalado na máquina gerenciada;
    - 1.8.4.5. Se o antivírus está atualizado;
    - 1.8.4.6. Nome do computador;
    - 1.8.4.7. Domínio ou grupo de trabalho do computador;
    - 1.8.4.8. Sistema operacional e Service Pack;
    - 1.8.4.9. Quantidade de memória RAM;
    - 1.8.4.10. Endereço IP;
- 1.9. Capacidade de instalar remotamente a solução de antivírus nas estações (endpoints) e servidores Windows, através de compartilhamento administrativo, login script e GPO do Microsoft Active Directory, no mínimo.
- 1.10. Capacidade de gerar pacotes auto-executáveis para a instalação do software para gerenciamento, além de automatização para instalação de todos módulos e informações necessárias para o funcionamento do produto (licenças, configurações, etc).
- 1.11. Capacidade de importar a estrutura do Microsoft Active Directory para a descoberta de máquinas da rede corporativa.
- 1.12. Capacidade de monitorar a rede, em diferentes sub redes, a fim de encontrar máquinas novas, para a instalação automática da solução de segurança.
- 1.13. Deve ser capaz de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem a necessidade de instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar o tráfego da rede.
- 1.14. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar o tráfego de link entre sites diferentes.
- 1.15. Deve permitir a herança de tarefas e políticas na estrutura de hierarquia de servidores administrativos.

- 1.16. Deve permitir que dispositivos gerenciados se conectem via Internet ao servidor de gerência, caso estejam fora da rede corporativa, sem a necessidade de utilização de recursos "em nuvem".
- 1.17. Capacidade de realizar atualização incremental de vacinas nos computadores clientes a partir da rede local e da Internet.
- 1.18. A atualização incremental de vacinas deve ser disponibilizada, no mínimo, com frequência diária.
- 1.19. A solução deve possuir integração com o Active Directory, de maneira a permitir a definição de políticas diferentes, baseadas em usuários ou grupos.
- 1.20. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
- 1.21. Deve armazenar histórico das alterações feitas em políticas;
- 1.22. Deve permitir a realocação de máquinas novas na rede para um determinado grupo utilizando os seguintes parâmetros:
  - 1.22.1. Nome do computador;
  - 1.22.2. Nome do domínio;
  - 1.22.3. Range de IP;
  - 1.22.4. Sistema Operacional;
  - 1.22.5. Máquina virtual.
- 1.23. Caso a solução ofertada não atenda na totalidade os itens aqui referidos, será permitido a composição com outras soluções a fim de atender na plenitude dos itens aqui descritos.
- 1.24. Deve possuir uma base de inteligência global, do próprio fabricante, sobre campanhas de ameaças existentes;
- 1.25. Deve ser capaz de dar visibilidade sobre campanhas de ameaças globais com segregação por vertical de negócio;
- 1.26. Deve ser capaz de dar visibilidade sobre campanhas de ameaças globais com segregação por país, incluindo o Brasil;
- 1.27. A solução deve ser capaz de proporcionar a busca em campanhas globais por ameaças baseadas em nome e/ou IOCs;
- 1.28. Deve ser capaz de indicar quantos e quais dispositivos dentro da empresa estão vulneráveis a uma determinada campanha;
- 1.29. Deve ser capaz de mostrar o nível de postura de segurança da organização, em relação às campanhas de ameaças globais identificadas na base de inteligência do fabricante;
- 1.30. Deve ser capaz de propor procedimentos de mitigação dos riscos de segurança nos endpoints referentes a campanhas de ameaças específicas;
- 1.31. Cada campanha identificada pela solução deverá possuir as seguintes informações:
  - 1.31.1. Descrição;
  - 1.31.2. IOCs;
  - 1.31.3. Detalhes do Impacto no ambiente;
  - 1.31.4. Prevalência Global;
  - 1.31.5. Endpoints afetados.
  - 1.31.6. Comportamento da ameaça.

1.32. Deve ser capaz de identificar em cada campanha de ameaça as técnicas utilizadas, relacionadas e mapeadas ao MITRE Framework.

## **2. Item 1 – Licença de software de segurança para estações de trabalho e servidores.**

### **2.1. Requisitos Gerais**

- 2.1.1. Prover segurança para as estações de trabalho (endpoints), sejam físicas ou em ambiente virtualizado.
- 2.1.2. Se comunicar com console central de gerenciamento, de forma que seja possível gerenciar todas as funcionalidades.
- 2.1.3. Detectar e eliminar programas maliciosos (malwares), tais como vírus, ransomware, spywares, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros.
- 2.1.4. Identificar e proteger contra eventuais vulnerabilidades dos sistemas operacionais e aplicações;
- 2.1.5. Deve detectar e eliminar, de forma automática e em tempo real, programas maliciosos em:
  - 2.1.5.1. Processos Em Execução Em Memória principal (RAM);
  - 2.1.5.2. Arquivos Executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);
  - 2.1.5.3. Arquivos Compactados, pelo menos nos seguintes formatos: ZIP, EXE, ARJ, RAR, e CAB.
  - 2.1.5.4. Detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex;
- 2.1.6. Capacidade de detecção heurística de malwares desconhecidos.
- 2.1.7. Possuir tecnologia de Machine Learning de pre-execution, run time machine e post-execution;
- 2.1.8. Deve prover, no mínimo, as seguintes proteções:
  - 2.1.8.1. Antivírus de arquivos;
  - 2.1.8.2. Antivírus web (verificação de sites e downloads contra malwares);
  - 2.1.8.3. Firewall de host com HIPS (Host Intrusion Prevention System);
  - 2.1.8.4. Proteção contra ataques aos serviços/processos do antivírus;
  - 2.1.8.5. Controle de dispositivos;
  - 2.1.8.6. Controle de execução de aplicativos;
  - 2.1.8.7. Controle de acesso a sites por categorias (Adulto, Jogos, etc);
  - 2.1.8.8. Prevenção contra exploração de vulnerabilidades;
  - 2.1.8.9. Capacidade de integração com a AntimalwareScan Interface (AMSI).
- 2.1.9. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

### **2.2. Detalhamento das proteções:**

- 2.2.1. Antivírus de arquivos:

- 2.2.1.1. Verificar todos os arquivos criados, acessados ou modificados, inclusive em sessões de linha de comando (DOS ou shell) abertas pelo usuário;
- 2.2.1.2. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;
- 2.2.1.3. Deve possuir Módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
- 2.2.1.4. Deve possuir Módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, sendo possível personalizar chaves específicas para serem monitoradas ou bloqueadas;
- 2.2.1.5. Capacidade para definir escopo de varredura/rastreamento: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos
- 2.2.1.6. Capacidade de adicionar pastas/arquivos em uma zona de exclusão, a fim de excluí-los da verificação.
- 2.2.1.7. Possibilidade de definir frequência de varredura: horária, diária, semanal e mensal;
- 2.2.1.8. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias.
- 2.2.1.9. Capacidade de realizar a verificação "inteligente" de arquivos, ou seja, somente verificará o arquivo se este for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la apenas a partir da extensão do arquivo.
- 2.2.1.10. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
- 2.2.2. Antivírus web:
  - 2.2.2.1. O antivírus web deve ter a capacidade de verificação de tráfego HTTP/HTTPS e scripts (JavaScript, Visual Basic Script, etc.).
  - 2.2.2.2. Capacidade de limitar o acesso a sites da internet por reputação.
  - 2.2.2.3. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus web;
  - 2.2.2.4. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Google Chrome;
- 2.2.3. Firewall de host com HIPS (Host Intrusion Prevention System)
  - 2.2.3.1. O módulo de firewall deve conter, no mínimo, dois conjuntos de regras:
    - 2.2.3.1.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
    - 2.2.3.1.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo terá acesso à rede.

- 2.2.3.2. Deve possuir módulo HIPS (Host Intrusion Prevention System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.
- 2.2.4. Proteção contra Ameaças Avançadas
  - 2.2.4.1. A solução deve permitir o confinamento dinâmico de aplicativos e arquivos executáveis com indícios maliciosos (Ransomware)
  - 2.2.4.2. A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executando-as em ambiente controlado;
  - 2.2.4.3. Deve permitir a indicação de aplicações confiáveis para que não caiam no filtro de confinamento dinâmico;
  - 2.2.4.4. Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada
  - 2.2.4.5. Solução deve manter um cache de reputação local com informações de aplicações - conhecidas, desconhecidas e maliciosas.
  - 2.2.4.6. Dentre os comportamentos maliciosos, deve ser capaz de:
    - 2.2.4.6.1. Bloquear acesso local a partir de cookies;
    - 2.2.4.6.2. Bloquear criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs;
    - 2.2.4.6.3. Bloquear criação de arquivos em qualquer local de rede;
    - 2.2.4.6.4. Bloquear criação de novos CLSIDs, APPIDs e TYPELIBs;
    - 2.2.4.6.5. Bloquear criação de threads em outro processo;
    - 2.2.4.6.6. Bloquear a desativação de executáveis críticos do sistema operacional;
    - 2.2.4.6.7. Leitura/Exclusão/Gravação de arquivos visados por Ransomwares;
    - 2.2.4.6.8. Gravação e Leitura na memória de outro processo;
    - 2.2.4.6.9. Bloqueio de Modificação da política de firewall do Windows;
    - 2.2.4.6.10. Bloqueio de Modificação da pasta de tarefas do Windows;
    - 2.2.4.6.11. Bloqueio de Modificação de arquivos críticos do Windows e Locais do Registro;
    - 2.2.4.6.12. Bloqueio de Modificação de arquivos executáveis portáteis;
    - 2.2.4.6.13. Bloqueio de Modificação de bit de atributo oculto;
    - 2.2.4.6.14. Bloqueio de Modificação de bit de atributo somente leitura;
    - 2.2.4.6.15. Bloqueio de Modificação de entradas de registro de DLL AppInit;
    - 2.2.4.6.16. Bloqueio de Modificação de locais do registro de inicialização;
    - 2.2.4.6.17. Bloqueio de Modificação de pastas de dados de usuários;
    - 2.2.4.6.18. Bloqueio de Modificação do local do Registro de Serviços;
    - 2.2.4.6.19. Bloqueio de Suspensão de um processo;
    - 2.2.4.6.20. Bloqueio de Término de outro processo.
  - 2.2.4.7. Dos comportamentos observados, deve ser possível bloquear ou apenas informar caso o mesmo ocorra.

- 2.2.4.8. Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem customizada.
- 2.2.4.9. O modo de ativação do confinamento dinâmico para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca antes visto pela solução;
- 2.2.4.10. Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário
- 2.2.4.11. A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção
- 2.2.4.12. Deve possuir capacidade de inspecionar arquivos suspeitos e detectar comportamentos maliciosos utilizando técnicas de "machine-learning";
- 2.2.5. Controle de dispositivos:
  - 2.2.5.1. Deve possuir módulo de controle de dispositivos, que permita o bloqueio e a ativação dos seguintes dispositivos, no mínimo:
    - 2.2.5.1.1. Discos de armazenamento locais;
    - 2.2.5.1.2. Dispositivos de comunicação USB (modems, telefones, etc.);
    - 2.2.5.1.3. Armazenamento Removível;
    - 2.2.5.1.4. Impressoras USB;
    - 2.2.5.1.5. CD/DVD-ROM;
    - 2.2.5.1.6. Dispositivos PCMCIA;
    - 2.2.5.1.7. Dispositivos COM e LPT;
    - 2.2.5.1.8. Leitores de cartões (SD, MemoryStick, etc.);
    - 2.2.5.1.9. Wi-Fi;
    - 2.2.5.1.10. Dispositivos Infravermelhos (IRDA);
    - 2.2.5.1.11. Dispositivos MP3 ou smartphones;
    - 2.2.5.1.12. Dispositivos Bluetooth.
    - 2.2.5.1.13. Câmeras e Scanners
  - 2.2.5.2. Capacidade de liberar o acesso a um dispositivo específico sem a necessidade de desabilitar a proteção ou da intervenção local na máquina do usuário.
  - 2.2.5.3. Capacidade de adicionar novos dispositivos por Class ID/Hardware ID.
- 2.2.6. Controle de execução de aplicativos:
  - 2.2.6.1. O módulo de controle de aplicações deve prover a capacidade de visibilidade sobre as aplicações executadas e aplicar o controle de execução imposto pela política;
  - 2.2.6.2. Deve ser capaz de realizar um inventário das estações de trabalho protegidas informando todos os executáveis e arquivos de script presentes.
  - 2.2.6.3. Como resultado do inventário, a solução deve armazenar o nome completo do arquivo, tamanho, checksum, tipo de arquivo, nome da aplicação e versão;

- 2.2.6.4. Ao detectar um executável, a solução deverá consultar a Solução de reputação de arquivos e compartilhamento de informações de segurança e esta deverá informar um nível de confiança;
- 2.2.6.5. Caso não seja possível efetuar comunicação com a Solução de reputação de arquivos e compartilhamento de informações de segurança, o módulo deve realizar consulta de reputação para o Centro de Inteligência do fabricante;
- 2.2.6.6. Deve ser possível criar uma imagem base para a criação de uma política geral;
- 2.2.6.7. Capacidade de trabalhar no modo adaptativo, ou seja, adaptando-se à novas aplicações instaladas na máquina;
- 2.2.6.8. A solução deverá permitir a realização de varreduras por demandas em máquinas para executar a blindagem de aplicativos;
- 2.2.6.9. Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA- 1).
- 2.2.6.10. A solução deve suportar as seguintes modalidades de proteção:
  - 2.2.6.10.1. Application Whitelisting: criação de uma lista de aplicações autorizadas que podem ser executadas no equipamento, onde todas as demais aplicações são impedidas de serem executadas.
  - 2.2.6.10.2. Application Blocking / Blacklisting: criação de uma lista de aplicações não autorizadas que não podem ser executadas.
  - 2.2.6.10.3. Memory Protection: monitoração e proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em memória.
- 2.2.6.11. Solução suporta criação, configuração e manutenção de Whitelist dinamicamente através de definição de regras de confiança.
- 2.2.6.12. Deve ser capaz de proteger em modo standalone - online ou offline;
- 2.2.6.13. Além de possuir um conjunto de regras, deve permitir por parte do administrador que este customize-as de forma a adaptar a necessidade do órgão;
- 2.2.6.14. Deve suportar o uso de variáveis de ambiente para a criação de regras de monitoramento (Exemplo: %HOMEPATH%, %HOMEDRIVE%, %USERPROFILE%, %APPDATA%)
- 2.2.6.15. Deve suportar variáveis de ambiente em sistemas 64-bits (Exemplo: %PROGRAMFILES (x86)%)
- 2.2.6.16. Deve possibilitar o controle e bloqueio da instalação de ActiveX nas estações de trabalho.
- 2.2.6.17. Permitir o bloqueio de aplicações e os processos que a aplicação interage
- 2.2.6.18. Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não.
- 2.2.6.19. Permitir monitoração de Hooking de aplicações onde se podem determinar quais processos podem ser executados ou não.

2.2.7. Proteção contra ransomwares:

- 2.2.7.1. Bloquear a criptografia de arquivos em recursos compartilhados a partir de um processo malicioso, inclusive, que esteja sendo executado em outra máquina;
- 2.2.7.2. Monitoramento de pastas compartilhadas no ambiente Windows, rastreando o estado dos arquivos armazenados e os protegendo;
- 2.2.7.3. Na detecção de atividade maliciosa de criptografia por ransomware, o antivírus deve interromper o processo de criptografia e restaurar os arquivos ao seu estado original, impedindo a perda de dados corporativos.

**2.3. Características do módulo de reputação de arquivos e compartilhamento de informações de segurança:**

- 2.3.1. Deve ser fornecida em formato de appliance virtual.
- 2.3.2. O appliance virtual deve ser compatível no mínimo com ambiente virtualizado VMWare ESX.
- 2.3.3. A solução deve possuir capacidade de criar uma reputação local ou utilizar uma já existente em nuvem através da catalogação de todos os executáveis existentes no ambiente;
- 2.3.4. O servidor de orquestração deverá habilitar a troca de informação de ameaças entre os endpoints e servidores protegidos.
- 2.3.5. Este módulo deverá habilitar um protocolo de troca de informações de ameaças que permita o intercâmbio de informações entre soluções do mesmo fabricante e de fabricantes terceiros;
- 2.3.6. A troca de informação de ameaças deve se dar por meio de protocolo performático;
- 2.3.7. De forma a permitir menor impacto na rede, para tal método de consulta dos clientes a base de dados poderá ser síncrona ou assíncrona;
- 2.3.8. A solução deverá apresentar a reputação dos arquivos definida para cada um dos ativos conectados, dentre eles:
  - 2.3.8.1. Reputação local
  - 2.3.8.2. Reputação do centro de inteligência
- 2.3.9. Caso o arquivo tenha como origem a Internet, a solução deverá ser capaz de informar a partir de qual URL o arquivo foi obtido e a reputação desta última;
- 2.3.10. Deve ser possível realizar uma pesquisa do arquivo em base de conhecimento de terceiros (exemplo: Virus Total);
- 2.3.11. Após análise pela solução o administrador deve ter a possibilidade de:
  - 2.3.11.1. Rastrear em quais estações o arquivo foi executado;
  - 2.3.11.2. Identificar o arquivo como confiável;
  - 2.3.11.3. Identificar o arquivo como desconhecido;
  - 2.3.11.4. Identificar o arquivo como malicioso
  - 2.3.11.5. Analisar o certificado associado ao arquivo;
  - 2.3.11.6. Identificar o certificado associado como confiável ou malicioso;
- 2.3.12. Para minimizar o impacto a solução deve ter a capacidade de ser ativada no modo de observação nos endpoints e servidores protegidos;

- 2.3.13. Deve ser possível bloquear a execução de arquivos nunca antes vistos ou suspeitos no ambiente e informar o usuário por meio de mensagem.
- 2.3.14. Deve ser capaz de identificar manualmente um arquivo como malicioso impedindo sua execução no ambiente;
- 2.3.15. Deve ser gerenciado pela mesma console de gerenciamento da solução de proteção de endpoints e servidores.

#### **2.4. Módulo de proteção para dispositivos móveis**

- 2.4.1. A solução de "Proteção para dispositivos móveis", deve proteger a CONTRATANTE contra as ameaças em dispositivos móveis, Android e IOS, incluindo malwares, ameaças de rede, identificação de vulnerabilidades e defesa física dos dispositivos. O objetivo principal desta solução é proteger os usuários móveis, impedindo que ameaças nestes dispositivos possam impactar nos serviços e na rede da CONTRATANTE.
- 2.4.2. Características Gerais:
  - 2.4.2.1. Deverá ser ofertado como um serviço on-premises (local) ou em console baseada em nuvem de forma a garantir suas funcionalidades independente da rede que o dispositivo estiver conectado;
  - 2.4.2.2. A solução deverá possuir console WEB para administração da solução;
  - 2.4.2.3. Possuir dashboard com os principais indicadores da solução, como Distribuição de níveis de risco, dispositivos em não conformidade, total de dispositivos protegidos e incidentes recentes;
  - 2.4.2.4. Apresentar, nos dashboards, uma visão geral dos riscos examinados nos dispositivos móveis, como ameaças de rede, vulnerabilidades e malwares encontrados;
  - 2.4.2.5. Deverá possuir uma apresentação gráfica referente às informações dos dispositivos registrados na solução;
  - 2.4.2.6. A console deverá apresentar os principais incidentes gerados, contendo todos os detalhes sobre o mesmo e o dispositivo que gerou o incidente;
  - 2.4.2.7. A solução deverá apresentar um relatório de ações recomendadas, para que com tais dados os administradores da solução possam criar ações para melhorar a segurança dos dispositivos móveis da CONTRATANTE;
  - 2.4.2.8. A solução deverá ser categorizada como uma solução de MTD (Mobile ThreatDefense);
  - 2.4.2.9. Deverá ser compatível com os sistemas operacionais IOS e Android;
  - 2.4.2.10. O cliente da solução deverá estar disponível nas lojas oficiais dos fabricantes, sendo Apple Store para IOS e Google Play para Android;

- 2.4.2.11. Permitir configuração no cliente instalado nos dispositivos móveis para que nenhuma informação e alertas seja visível para o usuário final, através de modo não interativo;
- 2.4.2.12. Deverá possuir as seguintes características mínimas de proteção:
  - 2.4.2.12.1. Proteção contra Malwares:
    - 2.4.2.12.1.1. Proteção em tempo real contra malwares conhecidos e desconhecidos;
    - 2.4.2.12.2. Defesa física
      - 2.4.2.12.2.1. Identificação de upgrades do sistema operacional;
      - 2.4.2.12.2.2. Identificação de dispositivo com root;
- 2.4.2.13. Deverá possuir integração com solução de SIEM de mercado;
- 2.4.2.14. A solução deve apresentar notificações de violações para o usuário final e para os administradores da solução, através de Email e Notificações Push;

### **2.5. Compatibilidade:**

- 2.5.1. O software de segurança deve ser compatível com as seguintes versões de sistemas operacionais Windows para estações de trabalho:
  - 2.5.1.1. Microsoft Windows 8 (e suas edições);
  - 2.5.1.2. Microsoft Windows 8.1 (e suas edições);
  - 2.5.1.3. Microsoft Windows 10 (e suas edições);
- 2.5.2. O software de segurança deve ser compatível com as seguintes versões de sistemas operacionais Windows para servidores:
  - 2.5.2.1. Microsoft Windows Server 2012 (e suas edições);
  - 2.5.2.2. Microsoft Windows Server 2012 R2 (e suas edições);
  - 2.5.2.3. Microsoft Windows Server 2016 (e suas edições);
  - 2.5.2.4. Microsoft Windows Server 2019 (e suas edições);
- 2.5.3. O software de segurança deve ser compatível para a funcionalidade de antimalware, no mínimo, com a seguinte distribuição/versão de sistema operacional Linux para estações de trabalho:
  - 2.5.3.1. Red Hat Enterprise 6.x, 7.x e 8.x, 64bits;
  - 2.5.3.2. SUSE Linux Enterprise Server 12.x e 15.x, 64bits;
  - 2.5.3.3. Ubuntu 16.04, 18.04, 19.10, 64bits;
  - 2.5.3.4. CentOS 6.x, 7.x e 8.x, 64bits;
  - 2.5.3.5. Oracle Linux 6, 7 e 8, 64bits;
  - 2.5.3.6. Amazon Linux 64bits;

## **3. Item 2 – Licença de software para ambientes virtualizados.**

### **3.1. Requisitos Gerais**

- 3.1.1. Ser totalmente compatível e homologada para gerenciamento de máquinas virtuais nos ambientes VMware e Hyper-V;
- 3.1.2. Deverá ter a disponibilidade de ser integrado com o VMWare através do VMWare NSX e oferecer escaneamento sem instalar o produto na máquina virtual;

- 3.1.3. Deve prover, no mínimo, as seguintes proteções:
  - 3.1.3.1. Antivírus de arquivos que verifique todos os arquivos criados, acessados ou modificados;
  - 3.1.3.2. Proteção contra ataques aos serviços/processos do antivírus;
- 3.1.4. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na remota.
- 3.1.5. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
  - 3.1.5.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
  - 3.1.5.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
  - 3.1.5.3. Leitura de configurações;
  - 3.1.5.4. Modificação de configurações;
- 3.1.6. Em caso de erros, deve ter a capacidade de criar logs e traces automaticamente, sem necessidade de uso de outros softwares.
- 3.1.7. Capacidade de adicionar pastas/arquivos em uma zona de exclusão, a fim de excluí-los da verificação.
- 3.1.8. Capacidade de realizar a verificação "inteligente" de arquivos, ou seja, somente verificará o arquivo se este for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não a tomar apenas a partir da extensão do arquivo.
- 3.1.9. Capacidade de verificar objetos usando heurística.
- 3.1.10. Antes de qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

### **3.2. Compatibilidade**

- 3.2.1. O software de segurança deve ser compatível com as seguintes versões de sistemas operacionais Windows para estações servidoras:
  - 3.2.1.1. Microsoft Windows Server 2012 (e suas edições);
  - 3.2.1.2. Microsoft Windows Server 2012 R2 (e suas edições);
  - 3.2.1.3. Microsoft Windows Server 2016 (e suas edições);
  - 3.2.1.4. Microsoft Windows Server 2019 (e suas edições);
- 3.2.2. O software de segurança deve ser compatível, no mínimo, com as seguintes distribuições/versões de sistemas operacionais Linux para servidores:
  - 3.2.2.1. RedHat Enterprise Linux 6.7 Server, ou superior;
  - 3.2.2.2. SUSE Linux Enterprise Server 12 SP1, ou superior;
  - 3.2.2.3. Ubuntu 14.04 LTS ou superior;

## **4. Item 3 -Serviço de implantação e migração da solução para proteção de endpoints e servidores**

- 4.1. A LICITANTE vencedora será inteiramente responsável pela instalação, atualização ou migração da solução antivírus atualmente em uso pela CONTRATANTE, bem como às despesas diretas ou indiretas para execução das atividades pela sua equipe técnica;

- 4.2. A instalação, atualização ou migração dos softwares em estações de trabalho poderá ser realizada remotamente, sem causar indisponibilidade do ambiente, devendo ser realizada em horários a serem definidos pela CONTRATANTE;
- 4.3. A instalação, atualização ou migração dos softwares em servidores de rede poderá ser realizada remotamente, devendo ser realizada em horários a serem definidos pela CONTRATANTE;
- 4.4. A CONTRATANTE poderá autorizar a instalação, atualização ou migração durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento de sua rede de computadores e serviços em produção;
- 4.5. O processo de instalação, atualização ou migração da solução deverá ser acompanhado por analistas da CONTRATANTE;
- 4.6. Para garantir que a instalação, atualização ou migração não afetará o ambiente da CONTRATANTE, os procedimentos e atividades deverão ser realizados por técnicos certificados pelo fabricante.
- 4.7. Em caso de migração de solução, a CONTRATADA deverá:
  - 4.7.1. Realizar a migração de todas as políticas, regras e customizações configuradas no CONTRATANTE;
  - 4.7.2. A CONTRATADA deverá se reunir com a equipe técnica da CONTRATANTE e elaborar um plano de migração, contendo as etapas, modelos, arquiteturas, funcionalidades e configurações da solução que serão implantadas durante a execução do serviço de migração.
  - 4.7.3. A Migração da solução deverá seguir todos os procedimentos internos do CONTRATANTE, incluindo os processos de registro de mudanças, liberações e incidentes.

#### 5. **Item 4 - Treinamento e Atualização Tecnológica**

- 5.1. A CONTRATADA deverá fornecer treinamento com carga horária mínima de **20 (vinte) horas**, contemplando a perfeita instalação, operação, manuseio, gerenciamento, configuração e utilização das soluções contratadas;
- 5.2. Os treinamentos deverão ser realizados em dias úteis, em horário comercial;
- 5.3. O treinamento **deverá ser realizado de forma remota**;
- 5.4. Deverá ser disponibilizado material didático impresso e/ou em mídia, sem custo adicional para a CONTRATANTE. Todo material deverá estar, preferencialmente, em língua portuguesa (Brasil), sendo aceitável o idioma inglês;
- 5.5. Deverá ser emitido certificado de participação ao final do curso a cada participante;
- 5.6. O cronograma efetivo do treinamento será definido em conjunto com a CONTRATANTE, após a assinatura do contrato;
- 5.7. Caso o treinamento/atualização fornecido não for satisfatório, mediante avaliação tempestiva e fundamentada, tanto em relação à qualidade ou à carga horária efetiva, a CONTRATADA deverá realizá-los novamente, sem ônus adicional à CONTRATANTE;
- 5.8. A critério da CONTRATANTE, o treinamento poderá ser dividido em turmas;
- 5.9. O conteúdo programático deverá englobar, pelo menos, os seguintes assuntos:
  - 5.9.1. Instalação do ambiente;
  - 5.9.2. Manutenção básica, intermediária e avançada;
  - 5.9.3. Configurações básicas e avançadas;



ABOUTNET INFORMATICA LTDA - EPP  
C.N.P.J.: 07.751.724/0001-16  
I.E. 799.118.325.112  
Fone/Fax: 11 5612 8200

Verificação de alertas e er

Nos preços ofertados estão incluídos todos os custos diretos e indiretos (frete, seguro, imposto e taxas, etc.) e quaisquer outras despesas com incidam ou venham a incidir sobre o objeto desta proposta.


A proposta está em conformidade com as especificações fornecidas, estimando-se os preços unitários e total.

Prazo de entrega: 30 dias

VALIDADE DA PROPOSTA: 90 Dias

Condições de pagamento: 30 (trinta) dias após o aceite das Notas Fiscais

Atenciosamente,



---

AboutNet Informática Ltda - EPP  
Álvaro Alves

\*\*\*\*Empresa Optante Pelo Simples Nacional\*\*\*\*



## **AO Tribunal Regional do Trabalho da 13ª Região**

**Att:** Sr. Raimundo José Campos Jr.

**REF:** Fornecimento de Solução Antivírus McAfee Endpoint pelo período de 48 (quarenta e oito) meses, contemplando serviços de manutenção, atualização, garantia e suporte técnico.

### Apresentação da Empresa

A XSITE é uma empresa atuante no mercado de Segurança da Informação e Desenvolvimento de Projetos de TI. A nossa missão é oferecer soluções tecnológicas inovadoras e que suportem aos requisitos da LGPD. Soluções alinhadas com as estratégias de atuação da empresa, que impulsionem o negócio do cliente e o ajudem a expandir o seu horizonte de atuação.

Para atingir este objetivo a empresa investe permanentemente no seu capital humano, contando com um quadro de pessoas competentes, qualificadas e comprometidas com o resultado e a qualidade dos serviços prestados.

### Da McAfee

As soluções da McAfee são projetadas para funcionarem juntas, integrando a proteção contra vírus, *malware* e *spyware* com recursos de gerenciamento de segurança que proporcionam análise e visibilidade insuperáveis em tempo real, reduzindo os riscos, garantindo a conformidade e ajudando as empresas a alcançarem o máximo das eficiências operacionais.

As tecnologias de segurança da *McAfee* usam um recurso prognóstico único que utiliza a premiada equipe de pesquisas do *McAfee Global Threat Intelligence*, permitindo que os usuários domésticos e as empresas permaneçam à frente das ameaças on-line.

Os produtos e soluções de segurança da *McAfee* abrangem as seguintes áreas:

- Proteção de dados
- Segurança de banco de dados
- Segurança de e-mail e da Web
- Proteção de terminais
- Segurança móvel
- Segurança de rede
- Risco e Conformidade
- Segurança Como Serviço (Security SaaS)
- Gestão de Segurança

Contando ainda com o *McAfee GTI - Global Threat Intelligence*, as soluções da *McAfee* ajudam as empresas a melhorar a visibilidade da sua postura de segurança, permitindo que as empresas

adotem a tecnologia da Web 2.0, virtualização, computação na nuvem e dispositivos móveis e pessoais, protegendo ao mesmo tempo os ativos essenciais e os dados confidenciais.

O **McAfee Global Threat Intelligence (GTI)** avisa sobre comportamento anormal e antecipadamente ajusta a reputação do site para que os produtos de segurança da web da **McAfee** possam bloquear o acesso e proteger os clientes. Em seguida, o **McAfee** GTI observa atentamente por meio de sua ampla proteção de rede de sensores e conecta os pontos entre o site e o *malware*, as mensagens de e-mail, os endereços IP associados e outras conexões, ajustando a reputação de cada entidade relacionada, para que os produtos de segurança da **McAfee** possam proteger os usuários de ameaças cibernéticas por todos os ângulos. O **McAfee** GTI oferece a mais abrangente proteção contra ameaças do mercado.

Com a visibilidade em todos os principais vetores de ameaça – arquivos, web, mensagens e rede – e a visualização das vulnerabilidades mais recentes no setor de TI, a **McAfee** correlacionou dados reais coletados de milhões de sensores instalados em todo o mundo e oferece proteção instantânea e muitas vezes antecipada por meio de seus produtos de segurança.





## Dos Investimentos

Item	Descrição	QTDE	Valor Unitário (R\$)	Preço Total 48 meses (R\$)
<b>Lote Único</b>				
1	Licença de software de segurança para estações de trabalho (endpoints) e servidores + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por 48 meses.	82.809	237,06	R\$ 19.630.701,54
2	Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por 48 meses.	5.139	R\$ 398,82	R\$ 2.049.535,98
3	Implantação e configuração da solução + Repasse de conhecimento hands-on	28	R\$ 27.820,00	R\$ 778.960,00
4	Treinamento EAD de capacitação técnica para administração da solução.	189	R\$ 4.151,60	R\$ 768.046,00
<b>VALOR TOTAL PARA O LOTE</b>				R\$ 23.227.243,52

O valor total da proposta é de R\$ 23.227.243,52 (vinte e três milhões duzentos e vinte e sete mil duzentos e quarenta e três reais e cinquenta e dois centavos).

A validade desta proposta é de 90 (noventa dias).

Prazo de entrega de 30 dias.

Atenciosamente,

João Gualberto Rizzo Araujo  
Diretor

Razão Social: Centro de Pesquisas em Informática Eireli

CNPJ: 40.584.096/0001-05

Nome Fantasia: XSITE Consultoria e Tecnologia

Telefone - (71)3018-7284

E-mail: [jgra@xsite.com.br](mailto:jgra@xsite.com.br)



Nova Lima, 17 de maio de 2021.

Á Tribunal Regional do Trabalho da 13ª Região

A/C: Raimundo Campos

Prezado Senhor,

Vimos apresentar a nossa proposta comercial para aquisição da solução de Proteção de Endpoint Sophos , conforme descrição abaixo. A licença de Uso é valida com 48 meses de manutenção.

Item / Serviço	Quantidade	Valor Unitário	Valor Total
Central Intercept X Advanced with EDR	82.809	R\$ 446,80	R\$ 36.999.061,20
Central Intercept X Advanced with EDR <b>Server</b>	5.139	R\$ 254,72	R\$ 1.309.006,08
Implantação e configuração da solução + Repasse de conhecimento hands-on	28	R\$ 40.000,00	R\$ 1.120.000,00
Treinamento EAD de capacitação técnica para administração da solução	189	R\$ 3.100,00	R\$ 585.900,00
<b>Valor Total da Proposta:</b>		<b>R\$ 40.013.968,00</b>	

**Validade da proposta:** 30 dias

**Prazo de Entrega:** Em até 20 (vinte) dias após o recebimento da ordem de compra.

**Forma de pagamento:** 30 (trinta) dias.

Atenciosamente,  
Aparecida C. Lemos  
Sócia Administradora  
Tel: +55 31 3241-7083  
[adik@adik.com.br](mailto:adik@adik.com.br)  
[www.adik.com.br](http://www.adik.com.br)

Adik Software Ltda  
CNPJ: 41.676.438/0001-71 Inscrição Estadual: 783.781.599-0092  
Alameda Oscar Niemayer 1033 sala 202 – Vila da Serra – Nova Lima – MG – CEP 34.006-065  
Tel / Fax: + 55 313241-7083  
[www.adik.com.br](http://www.adik.com.br) [adik@adik.com.br](mailto:adik@adik.com.br)



Brasília, 14 de maio de 2021.

Ao

**TRT-13****Ref. Proposta 02-093**

Na qualidade de empresa parceira e revendedora de soluções de segurança da informação, apresentamos cotação dos produtos abaixo:

O Symantec Endpoint Protection é uma solução cliente-servidor que protege laptops, desktops e servidores em sua rede contra malwares, riscos e vulnerabilidades. O Symantec Endpoint Protection possui proteção contra vírus e proteções avançadas contra ameaças, protegendo proativamente seus computadores contra ameaças conhecidas e desconhecidas, como vírus, worms, cavalos de Tróia e adwares. O Symantec Endpoint Protection oferece proteção até mesmo contra ataques mais sofisticados que escapam das medidas de segurança tradicionais, como rootkits, ataques de dia zero e spywares.

O Symantec Endpoint Protection (SEP) requer uma licença para receber as atualizações de segurança, atualizações do produto e acesso ao suporte técnico. Após a instalação do Symantec Endpoint Protection, você possui 60 dias para adquirir as licenças necessárias.

Lote	Item	Descrição	QTD	V. UNIT	V.TOTAL
1	1	Licença de software de segurança para estações de trabalho (endpoints) e servidores + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por 48 meses.	82809	R\$ 242,12	R\$ 20.049.715,08
	2	Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por 48 meses.	5139	R\$ 269,89	R\$ 1.386.964,71
	3	Implantação e configuração da solução + Repasse de conhecimento hands-on	28	R\$ 31.210,00	R\$ 873.880,00
	4	Treinamento EAD de capacitação técnica para administração da solução.	189	R\$ 6.157,79	R\$ 1.163.822,31
Valor Total					R\$ 23.474.382,10

**Validade da proposta:** 30 dias**Forma de Pagamento:** 30 dias após a entrega das licenças e Nota Fiscal.



**Denis Silva**

Gerente de Contas

[Denis.Silva@fasthelp.com.br](mailto:Denis.Silva@fasthelp.com.br)

(61) 9 9330-7361

(61) 3363-8636

## CONDIÇÕES GERAIS

1. A não efetivação do pagamento na forma e condições pactuadas nesta proposta acarretará a incidência de juros de 1% (um por cento) ao mês “pro rata temporis”, entre a data do vencimento e o dia do efetivo pagamento e multa moratória correspondente a 10% (dois por cento) do valor devido.
2. O título pago em atraso estará sujeito a **protesto** após 02 (dois) dias a contar do vencimento.
3. Quantia devida pelo (a) **ACEITANTE** à **PROPONENTE**, paga em atraso sem a inclusão de multa, juros e correção monetária não caracteriza obrigação cumprida/satisfeita, ficando a **PROPONENTE** autorizada a incluir os acréscimos devidos e não pagos no boleto bancário subsequente.
4. O atraso no pagamento por período igual ou superior a 30 (trinta) dias após o vencimento, poderá acarretar, independentemente de aviso ou notificação judicial ou extrajudicial, **a suspensão da prestação do serviço de suporte** a partir do trigésimo primeiro dia após o vencimento de qualquer valor que esteja em atraso.
5. O atraso no pagamento por período igual ou superior a 60 (sessenta) dias após o vencimento, **poderá acarretar a rescisão de pleno direito do presente instrumento e a consequente desinstalação da Solução** a partir do sexagésimo primeiro dia após o vencimento de qualquer valor que esteja em atraso, mediante intervenção da **PROMITENTE** junto ao **FABRICANTE**, independentemente de aviso ou notificação judicial ou extrajudicial. O (A) **ACEITANTE** declara-se ciente e desde já **autoriza a desinstalação da Solução no caso de inadimplência por período igual ou superior a 60 (sessenta) dias.**
6. O (A) **ACEITANTE** declara-se ciente de que em caso de inadimplência, a **PROPONENTE** poderá informar tal fato aos órgãos de proteção de crédito, tais como SPC, SERASA e outros mais existentes para essa

finalidade, ficando legitimada e autorizada a fazê-lo na hipótese de atraso igual ou superior a 30 (trinta) dias no pagamento de qualquer verba/valor decorrente da presente proposta.

7. A aprovação de crédito ocorrerá mediante prévia consulta.
8. As atividades de suporte técnico inclusas nesta proposta comercial estão relacionadas nas soluções ofertadas neste documento. Qualquer atividade (ou chamado técnico) fora deste escopo será cobrado o valor de R\$ 120,00 (cento e vinte reais) por hora trabalhada.

#### **PROGRAMA DE INTEGRIDADE FAST HELP**

1. Todas as obrigações assumidas nos termos do presente contrato são possíveis de execução específica, na forma do Código de Processo Civil, servindo este instrumento como título executivo extrajudicial.
2. A contratação das obrigações estabelecidas no presente instrumento atende aos interesses de ambas as PARTES, acarretando obrigações bilaterais e equitativas, reconhecendo serem tais obrigações perfeitamente condizentes e adequadas à sua capacidade de adimplemento, não podendo, em qualquer momento e sob qualquer hipótese, arguir eventos de onerosidade excessiva no desempenho das obrigações ora contratadas, atendendo aos princípios da boa-fé.
3. Declaram as PARTES que não possuem em sua cadeia produtiva a exploração de trabalho infantil, ou de trabalho em situação degradante, análoga à de trabalho escravo, tampouco se beneficiam ou coadunam com tais práticas. As PARTES declaram, ainda, que em sua cadeia produtiva atuam de modo a preservar o meio ambiente, buscando sempre o desenvolvimento sustentável, minimizando os efeitos nocivos e eventuais impactos que possam ser causados ao meio ambiente em razão de sua produção.
4. As PARTES se obrigam, sob as penas previstas neste instrumento e na legislação aplicável, a observar e cumprirem rigorosamente toda a legislação aplicável à prevenção e combate de corrupção, atividades ilícitas, lavagem de dinheiro e demais atos ilícitos análogos, incluindo (porém a tanto não se limitando) a Lei 12.846/2013 e quaisquer outros dispositivos que venham a vigor a respeito de referida matéria.
5. As PARTES declaram e garantem que não estão envolvidas ou irão se envolver, direta ou indiretamente, por seus representantes, administradores, diretores, conselheiros, sócios ou acionistas, assessores, consultores, parte relacionada, seus diretores, conselheiros, sócios ou acionistas, assessores ou consultores, durante o cumprimento das obrigações previstas neste contrato, em qualquer atividade ou prática que constitua uma infração aos termos das Leis Anticorrupção.
6. As PARTES declaram e garantem que não se encontram, assim como seus representantes, administradores, diretores, conselheiros, sócios ou acionistas, assessores, consultores, direta ou indiretamente: (i) sob investigação em virtude de denúncias de suborno e/ou corrupção; (ii) no curso de um processo judicial e/ou

administrativo ou foram condenados ou indiciados sob a acusação de corrupção ou suborno; (iii) listados em alguma entidade governamental, tampouco conhecidos ou suspeitos de práticas de terrorismo e/ou lavagem de dinheiro; (iv) sujeitos a restrições ou sanções econômicas e de negócios por qualquer entidade governamental; e (v) banidos ou impedidos, de acordo com qualquer lei que seja imposta ou fiscalizada por qualquer entidade governamental.

7. O não cumprimento por qualquer das PARTES das Leis Anticorrupção e/ou da Política Anticorrupção será considerada uma infração grave a este contrato e conferirá a outra PARTE o direito de, agindo de boa-fé, declarar rescindido imediatamente o presente contrato, sem qualquer ônus ou penalidade, sendo a PARTE infratora responsável pelas perdas e danos, nos termos da lei aplicável.
8. As PARTES, cada uma por sua vez, declaram que, direta ou indiretamente, não irão receber, transferir, manter, usar ou esconder recursos que decorram de qualquer atividade ilícita, bem como não irá contratar como empregado ou de alguma forma manter relacionamento profissional com pessoas físicas ou jurídicas envolvidas com atividades criminosas, em especial as Leis Anticorrupção, lavagem de dinheiro, tráfico de drogas e terrorismo.

A CONTRATANTE declara conhecer o Programa de Integridade (Compliance), o Manual de Integridade e o Código de Ética e Conduta da CONTRATADA, o qual está disponível em seu sítio eletrônico, bem como declara, ainda, no melhor do seu conhecimento, não estar envolvida em qualquer situação que configure descumprimento ao disposto no referido Código de Ética e Conduta da CONTRATANTE.



Sexta-feira, 14 de maio de 2021

# Tribunal Regional do Trabalho da 13<sup>a</sup> Região

## ISH TECNOLOGIA S/A

---

**Matriz:** Rua Judith Maria Tovar Varejão, nº 355 - Enseada do Suá - Vitória/ES - CEP 29050-360

**Filial RJ:** Av. Presidente Wilson, nº 231/9º andar - Centro - Rio de Janeiro/RJ – CEP 20030-021

**Filial MG:** Av. Getúlio Vargas, nº 887/Sala 401 - Funcionários – Belo Horizonte/MG – CEP 30112-020

**Filial DF:** SCN Quadra 01, Bloco F/Salas 102 a 104, Ed América Office Tower - Brasília/DF CEP 70711-905

**Filial SP:** Rua Surubim, nº 577/5o andar - Ed. Igarassu – Brooklin – São Paulo/SP CEP - 04571-050

**Integrasys:** Rua Alberto de Oliveira Santos, nº 42/Sala 1802, Edifício Pasteur – Centro, Vitória – ES – CEP: 29.010-364

*Conteúdo Confidencial – Proibida a reprodução sem prévia autorização da ISH Tecnologia S/A*



**A:**  
Tribunal Regional do Trabalho da 13ª Região

**Ref.:**  
Proposta Técnica e Comercial para Solução de Segurança de End-point

**Empresa proponente:**  
ISH TECNOLOGIA S/A.  
**Matriz:** Rua Judith Maria Tovar Varejão, 355  
Enseada do Suá – Vitória – ES - CEP 29050-360.  
CNPJ: 01.707.536/0001-04.  
Tel.: 55 27 3334 8900.  
Fax: 55 27 3334 8905.

**Prezado,**

A ISH Tecnologia, empresa especializada em soluções de datacenter, segurança, infraestrutura de tecnologia da informação, apresenta sua proposta técnica para prestação de serviços especializados de fornecimento de Rede sem fio.

As informações, requisitos e exigências apresentadas no pedido formal de proposta do Tribunal Regional do Trabalho da 13ª Região, foram cuidadosamente analisados pela ISH Tecnologia, de forma a obter-se o melhor entendimento possível das necessidades em questão visando à oferta de serviços de excelente qualidade e que atendam às expectativas e objetivos estratégicos da Tribunal Regional do Trabalho da 13ª Região

Agradecemos esta oportunidade e nos colocamos a disposição para contribuir de forma plena com os objetivos e metas da Tribunal Regional do Trabalho da 13ª Região. Da mesma maneira, estamos a disposição para sanar quaisquer dúvidas decorrentes desta, ou em relação aos demais serviços oferecidos em nossas áreas de atuação que também podem ser obtidas por meio de nosso endereço virtual <http://www.ish.com.br>.

Atenciosamente,

Hélio Ferreira da Silva Junior  
Executivo de Contas  
ISH Tecnologia S/A  
Helio.ferreira@ish.com.br

---

**Matriz:** Rua Judith Maria Tovar Varejão, nº 355 - Enseada do Suá - Vitória/ES - CEP 29050-360  
**Filial RJ:** Av. Presidente Wilson, nº 231/9º andar - Centro - Rio de Janeiro/RJ – CEP 20030-021  
**Filial MG:** Av. Getúlio Vargas, nº 887/Sala 401 - Funcionários – Belo Horizonte/MG – CEP 30112-020  
**Filial DF:** SCN Quadra 01, Bloco F/Salas 102 a 104, Ed América Office Tower - Brasília/DF CEP 70711-905  
**Filial SP:** Rua Surubim, nº 577/5o andar - Ed. Igarassu – Brooklin – São Paulo/SP CEP - 04571-050  
**Integrasy:** Rua Alberto de Oliveira Santos, nº 42/Sala 1802, Edifício Pasteur – Centro, Vitória – ES – CEP: 29.010-364



## ÍNDICE

1. IDENTIFICAÇÃO DESTE DOCUMENTO .....	3
2. ACORDO DE CONFIDENCIALIDADE.....	4
3. A ISH TECNOLOGIA .....	5
4. SOLUÇÃO PROPOSTA.....	6
5. DISPOSIÇÕES GERAIS .....	9
6. CONDIÇÕES COMERCIAIS.....	8

---

**Matriz:** Rua Judith Maria Tovar Varejão, nº 355 - Enseada do Suá - Vitória/ES - CEP 29050-360  
**Filial RJ:** Av. Presidente Wilson, nº 231/9º andar - Centro - Rio de Janeiro/RJ – CEP 20030-021  
**Filial MG:** Av. Getúlio Vargas, nº 887/Sala 401 - Funcionários – Belo Horizonte/MG – CEP 30112-020  
**Filial DF:** SCN Quadra 01, Bloco F/Salas 102 a 104, Ed América Office Tower - Brasília/DF CEP 70711-905  
**Filial SP:** Rua Surubim, nº 577/5o andar - Ed. Igarassu – Brooklin – São Paulo/SP CEP - 04571-050  
**Integrasys:** Rua Alberto de Oliveira Santos, nº 42/Sala 1802, Edifício Pasteur – Centro, Vitória – ES – CEP: 29.010-364



## 1. Identificação deste documento

<b>Número</b>	P2021051401-TRT13- Solução de Segurança de End-Point
<b>Título</b>	Solução de Segurança de End-Point
<b>Destinatário</b>	Raimundo José Campos Jr.
	(85)3533-6055
	rjcampos@trt13.jus.br
<b>Partes</b>	<b>NOMES:</b> Tribunal Regional do Trabalho da 13ª Região.
	<b>A ISH TECNOLOGIA S/A</b>
<b>Responsáveis Técnicos</b>	Vinicius Neves
	Arquiteto de soluções

**Matriz:** Rua Judith Maria Tovar Varejão, nº 355 - Enseada do Suá - Vitória/ES - CEP 29050-360  
**Filial RJ:** Av. Presidente Wilson, nº 231/9º andar - Centro - Rio de Janeiro/RJ - CEP 20030-021  
**Filial MG:** Av. Getúlio Vargas, nº 887/Sala 401 - Funcionários - Belo Horizonte/MG - CEP 30112-020  
**Filial DF:** SCN Quadra 01, Bloco F/Salas 102 a 104, Ed América Office Tower - Brasília/DF CEP 70711-905  
**Filial SP:** Rua Surubim, nº 577/5o andar - Ed. Igarassu - Brooklin - São Paulo/SP CEP - 04571-050  
**Integrasys:** Rua Alberto de Oliveira Santos, nº 42/Sala 1802, Edifício Pasteur - Centro, Vitória - ES - CEP: 29.010-364



## 2. Acordo de Confidencialidade

Todas as informações contidas neste documento são estritamente confidenciais e fornecidas com a finalidade, exclusiva, de descrever tecnicamente, a pedido do Tribunal Regional do Trabalho da 13ª Região, as soluções ISH e não deverão ser utilizadas para nenhuma outra finalidade. As informações, ideias, soluções e sugestões de projeto descritas neste documento, são de propriedade intelectual exclusiva da ISH.

Na hipótese de escolha de outro fornecedor, ou que não selecione nenhum num prazo de **30 dias** a contar da data desta proposta, o Tribunal Regional do Trabalho da 13ª Região, devolverá todas as informações exclusivas e confidenciais da ISH, não as utilizando nem revelando de nenhuma forma

O Tribunal Regional do Trabalho da 13ª Região, não publicará nem revelará estas informações, no todo ou em parte, sem permissão prévia e por escrito da ISH.

Relativamente aos dados e informações do CLIENTE a ISH declara que:

a) Salvo determinação judicial ou legal em contrário manterá as “Informações Confidenciais” em boa guarda e sigilo e não divulgará a qualquer pessoa física ou jurídica sem o consentimento expresso da contratante:

b) “**Informação Confidencial**” define-se como aquela assim explicitamente classificada.

c) Por solicitação do Tribunal Regional do Trabalho da 13ª Região, devolverá toda e qualquer Informação Confidencial.

d) As obrigações previstas sobre confidencialidade e sigilo sobreviverão ao relacionamento entre as partes, sendo que o sigilo das Informações Confidenciais permanecerá em vigor pelo prazo de 24 meses ou 2 anos contados a partir da data de rescisão do contrato.

Muitos dos nomes de empresas e serviços mencionados neste documento são marcas registradas. Todas elas são reconhecidas mediante esta declaração.



### 3. A ISH Tecnologia

Fundada em 1996, a ISH Tecnologia é uma empresa 100% brasileira que fornece soluções de Datacenter, Segurança da Informação e Infraestrutura de TI, atuando em todo o mercado nacional e na América Latina. A ISH conta com matriz, filiais e escritórios em Vitória/ES, São Paulo/SP, Brasília/DF, Belo Horizonte/MG e Rio de Janeiro/RJ.

Na década de 90 a internet ainda não era bem a internet como a vemos hoje, foi neste período que Al Gore cunhou um termo que descreveria o que estava por vir, algo como “uma rede de comunicação global de alta velocidade, por onde passariam dados, voz, vídeo e outras formas de informações por todo o mundo”. Para essa visão de rede ele deu o nome de Information Superhighway ou Super Rodovia da Informação.

O significado da sigla “ISH” vem dessa expressão, *Information Superhighway*, pois vivíamos nesse ambiente de tecnologia e já nessa época estávamos estruturando e implantando, ou seria “pavimentando”, arrojados projetos de infraestrutura e de segurança para essa “super rodovia”, inicialmente no Espírito Santo, depois em todos os estados brasileiros e América Latina.

A ISH ampliou seus horizontes executando projetos em todas as unidades da federação e em vários países de América Latina, conquistando um amplo portfolio de clientes, dos mais diversos segmentos de negócios, desde empresas multinacionais, governamentais, bancos, indústria e comércio, firmando parcerias tecnológicas com empresas de renome, oferecendo sempre a melhor solução a seus clientes e a evolução profissional de seus colaboradores.

#### 3.1. Parcerias



Figura 1 - Parceiros da ISH Tecnologia

**Matriz:** Rua Judith Maria Tovar Varejão, nº 355 - Enseada do Suá - Vitória/ES - CEP 29050-360  
**Filial RJ:** Av. Presidente Wilson, nº 231/9º andar - Centro - Rio de Janeiro/RJ - CEP 20030-021  
**Filial MG:** Av. Getúlio Vargas, nº 887/Sala 401 - Funcionários - Belo Horizonte/MG - CEP 30112-020  
**Filial DF:** SCN Quadra 01, Bloco F/Salas 102 a 104, Ed América Office Tower - Brasília/DF CEP 70711-905  
**Filial SP:** Rua Surubim, nº 577/5o andar - Ed. Igarassu - Brooklin - São Paulo/SP CEP - 04571-050  
**Integrasy:** Rua Alberto de Oliveira Santos, nº 42/Sala 1802, Edifício Pasteur - Centro, Vitória - ES - CEP: 29.010-364



## 4. Solução Proposta

Esta proposição contempla os serviços necessários para a Solução de Rede Wireless do TRIBUNAL REGIONAL DO TRABALHO DA 13ª REGIÃO – Confederação Nacional da Indústria, conforme descrito a seguir.

### 4.1. Solução

1	Licença de software de segurança para estações de trabalho (endpoints) e servidores + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por <b>48 meses</b> .	82.809
2	Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por <b>48 meses</b> .	5.139
3	Implantação e configuração da solução + Repasse de conhecimento hands-on	28
4	Treinamento EAD de capacitação técnica para administração da solução.	189

### 4.2. PREMISSAS, RESTRIÇÕES, LIMITES E NÃO ESCOPO

- a) A presente proposta não considera restrições de infraestrutura ou necessidade de execução de serviços ou aquisições/contratações de terceiros para compor o escopo de sua execução, se não acordadas explicitamente no seu conteúdo;
- b) Para acompanhamento da execução o CLIENTE deverá indicar expressamente colaborador de sua estrutura que possua autonomia para dirimir dúvidas, apontar prioridades de locais que sofrerão intervenção, desempenhando as atribuições de fiscal dos serviços;
- c) Para execução de atividades ou ações nas dependências do CLIENTE o mesmo se compromete em providenciar recursos de mobiliários, licenças de softwares não incluídos no escopo da presente proposta e outros recursos a serem identificados e apontados na agenda de kick-off do projeto;
- d) Não foram consideradas restrições de horários e agendas do CLIENTE, ou de sua equipe, para execução e acompanhamento das atividades do projeto;
- e) Link´s de Internet ou garantia mínima de banda para execução de configurações, downloads ou execução do escopo devem ser garantidos pelo CLIENTE, para as atividades que demandarem execução em suas dependências;

**Matriz:** Rua Judith Maria Tovar Varejão, nº 355 - Enseada do Suá - Vitória/ES - CEP 29050-360  
**Filial RJ:** Av. Presidente Wilson, nº 231/9º andar - Centro - Rio de Janeiro/RJ - CEP 20030-021  
**Filial MG:** Av. Getúlio Vargas, nº 887/Sala 401 - Funcionários - Belo Horizonte/MG - CEP 30112-020  
**Filial DF:** SCN Quadra 01, Bloco F/Salas 102 a 104, Ed América Office Tower - Brasília/DF CEP 70711-905  
**Filial SP:** Rua Surubim, nº 577/5o andar - Ed. Igarassu - Brooklin - São Paulo/SP CEP - 04571-050  
**Integrasy:** Rua Alberto de Oliveira Santos, nº 42/Sala 1802, Edifício Pasteur - Centro, Vitória - ES - CEP: 29.010-364



f) Em Projetos de venda de licença de antivírus a ISH não executa a instalação do produto em desktops (máquinas clientes), exceto para os casos em que tenha sido explicitamente contratada para esse fim;

g) A proposta não contempla, exceto se expressamente ajustada em seu texto, o fornecimento de licenças de Sistema Operacional de Servidores, não se responsabilizando, portanto, por sua instalação, atualização etc. Portanto, o CLIENTE é o responsável por entregar à equipe da ISH o equipamento servidor devidamente preparado para uso no projeto (instalado, configurado e atualizado);

h) Ratificamos que não faz parte do escopo do projeto o licenciamento de softwares necessários à execução do escopo negociado e que não tenham sido explicitamente incluídos na presente proposta.



## 5. Condições Comerciais

De acordo com o escopo desta proposta, apresentamos planilha orçamentária

Lote	Item	Descrição	QTD	V. UNIT	V.TOTAL
1	1	Licença de software de segurança para estações de trabalho (endpoints) e servidores + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por 48 meses.	82809	R\$ 226,28	R\$ 18.738.020,52
	2	Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por 48 meses.	5139	R\$ 226,28	R\$ 1.162.852,92
	3	Implantação e configuração da solução + Repasse de conhecimento hands-on	28	R\$ 32.000,00	R\$ 896.000,00
	4	Treinamento EAD de capacitação técnica para administração da solução.	189	R\$ 6.500,00	R\$ 1.228.500,00
<b>Valor Total</b>					<b>R\$ 22.025.373,44</b>

### 5.1. Prazos de Entrega

- O prazo de entrega estimado de Hardware / Software é de 60 (Sessenta) dias..
- O Prazo de entrega estimado de Serviços de suporte e operação é de 15 (Quise) dias.

### 5.2. Validade da Proposta

- Esta proposta tem validade de 60 (Sessenta) dias.

### 5.3. Forma de Pagamento

#### a) Hardware / Software e Garantias

- 100% do valor total dos equipamentos será faturado na data de sua entrega.

#### b) Serviços de Implantação, Consultoria e/ou Integração

- 50% do valor total dos serviços serão faturados no dia seguinte ao da realização de reunião de documentação de planejamento e 50% do valor total dos serviços

**Matriz:** Rua Judith Maria Tovar Varejão, nº 355 - Enseada do Suá - Vitória/ES - CEP 29050-360  
**Filial RJ:** Av. Presidente Wilson, nº 231/9º andar - Centro - Rio de Janeiro/RJ - CEP 20030-021  
**Filial MG:** Av. Getúlio Vargas, nº 887/Sala 401 - Funcionários - Belo Horizonte/MG - CEP 30112-020  
**Filial DF:** SCN Quadra 01, Bloco F/Salas 102 a 104, Ed América Office Tower - Brasília/DF CEP 70711-905  
**Filial SP:** Rua Surubim, nº 577/5o andar - Ed. Igarassu - Brooklin - São Paulo/SP CEP - 04571-050  
**Integrasy:** Rua Alberto de Oliveira Santos, nº 42/Sala 1802, Edifício Pasteur - Centro, Vitória - ES - CEP: 29.010-364



serão faturados no dia seguinte a entrega da documentação final (encerramento do projeto).

**c) Serviços Continuados Mensais (Suporte e/ou Monitoramento)**

- A fatura dos serviços continuados (mensais) será emitida no primeiro dia útil do mês subsequente ao da ativação dos serviços, sendo o primeiro pagamento *pro rata die*, contado a partir da ativação do serviço.

NOTA: O atraso ou a ausência de pagamento dos serviços e produtos contratados implicará na incidência de multa de 2% (dois por cento), além de juros de mora de 1% ao mês, a serem calculados *pro rata die* sobre o montante da dívida, desde o inadimplemento até a efetiva quitação do débito.

## 6. Disposições Gerais

1) No preço proposto, já estão incluídas todas e quaisquer despesas necessárias à perfeita execução do objeto, tais como: deslocamentos (viagens), hospedagem, alimentação, transporte, tributos, fretes, encargos sociais, seguros e demais despesas inerentes à execução do objeto e que estejam de acordo com o escopo do projeto e número de visitas e agendas necessárias ao desenvolvimento e implantação da solução.

2) Não estão incluídas despesas oriundas de agendas extemporâneas, não planejadas ou comunicadas com antecedência menor que 10 dias, as quais correrão às expensas do CLIENTE, desde que expressamente autorizadas.

3) A ISH TECNOLOGIA S/A se reserva o direito de, caso esta proposta seja aceita, firmar contrato e efetivar faturamento por qualquer uma das empresas do Grupo ISH, ou por uma de suas filiais, a saber:

- ISH ES – CNPJ 01.707.536/0001-04 – IE 082.338.035
- ISH RJ – CNPJ 01.707.536/0007-08 – IE 086.686.090
- ISH SP – CNPJ 01.707.536/0003-76 – IE 116.807.949.114
- ISH BSB – CNPJ 01.707.536/0004-57 – IE 0751.689.200.365
- ISH MG – CNPJ 01.707.536/0006-19 – IE 002.205.855.00-80
- INTEGRASYS – CNPJ 01.505.147/0001-04 – IE 082.129.54-1

4) O aceite desta proposta indica que o CLIENTE se compromete a não contratar funcionários da ISH Tecnologia S/A durante a execução dos serviços, bem como nos 12 (doze) meses subsequentes contados a partir do encerramento dos serviços ou contrato sob pena de multa equivalente ao montante de 120 (cento e vinte) vezes o valor do salário do profissional contratado.

---

**Matriz:** Rua Judith Maria Tovar Varejão, nº 355 - Enseada do Suá - Vitória/ES - CEP 29050-360  
**Filial RJ:** Av. Presidente Wilson, nº 231/9º andar - Centro - Rio de Janeiro/RJ – CEP 20030-021  
**Filial MG:** Av. Getúlio Vargas, nº 887/Sala 401 - Funcionários – Belo Horizonte/MG – CEP 30112-020  
**Filial DF:** SCN Quadra 01, Bloco F/Salas 102 a 104, Ed América Office Tower - Brasília/DF CEP 70711-905  
**Filial SP:** Rua Surubim, nº 577/5o andar - Ed. Igarassu – Brooklin – São Paulo/SP CEP - 04571-050  
**Integrasy:** Rua Alberto de Oliveira Santos, nº 42/Sala 1802, Edifício Pasteur – Centro, Vitória – ES – CEP: 29.010-364



5) Da mesma forma, a ISH Tecnologia S/A se compromete a não contratar funcionários do CLIENTE por igual período, sujeitando-se, portanto, às mesmas penalidades anteriormente mencionadas.

6) O prazo de duração do contrato será de **48 meses**, contados a partir da data de ativação dos serviços, podendo ser renovado automaticamente por iguais períodos, caso não haja manifestação de qualquer das partes, por escrito, com antecedência mínima de 30 dias do término do período vigente.

7) A **ATIVACÃO** marcará a disponibilidade dos serviços e o início do ciclo de faturamento. A **ATIVACÃO**, que poderá ser **TOTAL** ou **PARCIAL**, será comunicado formalmente à CONTRATANTE, que, por sua vez, disporá do prazo de 48 (quarenta e oito) horas para manifestar-se sobre eventual falha ou defeito na **ATIVACÃO DOS SERVIÇOS**. Decorrido tal período, não havendo manifestação da CONTRATANTE, serão considerados plenamente ativados os serviços e exigível o pagamento correspondente.

8) Esta **PROPOSTA COMERCIAL** vincula os contratantes. Caso o CLIENTE solicite a desistência antecipada e imotivada do contrato, após a assinatura da proposta comercial e antes da assinatura do contrato ou ativação dos serviços, o mesmo concorda que será plenamente aplicável a multa prevista no parágrafo único abaixo, utilizando como base para contagem de prazo contratual a data de assinatura da **PROPOSTA COMERCIAL** e/ou do contrato de prestação de serviços.

**Parágrafo Único:** A parte que solicitar a rescisão unilateral, por antecipação em relação ao prazo contratualmente fixado/renovado, deverá, obrigatoriamente, encaminhar a outra parte aviso prévio de 30 (trinta) dias, acerca de sua intenção em resolver o contrato, e incorrerá no pagamento de multa, de natureza não compensatória, sem prejuízo da responsabilidade por perdas e danos, nas seguintes hipóteses:

a) **Após o aceite da proposta e antes da assinatura do contrato:** multa equivalente à 10% do valor da proposta aceita e a o respectivo pagamento pelos investimentos já realizados até a data da solicitação, bem como dos serviços executados.

b) **Após a assinatura do contrato:** multa equivalente às condições previstas no instrumento contratual.

9) A redução das quantidades aceitas/contratadas de um mesmo serviço – denominada Downgrade – enseja a aplicação de multa conforme previsão do item acima.

10) Todos os valores contratados deverão ser reajustados 12 (doze) meses após a ativação do serviço ou com a periodicidade mínima definida por lei, de acordo com a variação do IPCA ou outro índice que venha substituí-lo.

**Matriz:** Rua Judith Maria Tovar Varejão, nº 355 - Enseada do Suá - Vitória/ES - CEP 29050-360

**Filial RJ:** Av. Presidente Wilson, nº 231/9º andar - Centro - Rio de Janeiro/RJ – CEP 20030-021

**Filial MG:** Av. Getúlio Vargas, nº 887/Sala 401 - Funcionários – Belo Horizonte/MG – CEP 30112-020

**Filial DF:** SCN Quadra 01, Bloco F/Salas 102 a 104, Ed América Office Tower - Brasília/DF CEP 70711-905

**Filial SP:** Rua Surubim, nº 577/5o andar - Ed. Igarassu – Brooklin – São Paulo/SP CEP - 04571-050

**Integrasys:** Rua Alberto de Oliveira Santos, nº 42/Sala 1802, Edifício Pasteur – Centro, Vitória – ES – CEP: 29.010-364



11) As responsabilidades das partes iniciarão a partir da assinatura da presente Proposta Comercial.

12) A assinatura do contrato definitivo é condição para que ocorra a ATIVAÇÃO DOS SERVIÇOS. Enquanto não assinado o contrato, os serviços permanecerão suspensos, sem prejuízo da multa e penalidades previstas neste instrumento.

---

**Matriz:** Rua Judith Maria Tovar Varejão, nº 355 - Enseada do Suá - Vitória/ES - CEP 29050-360  
**Filial RJ:** Av. Presidente Wilson, nº 231/9º andar - Centro - Rio de Janeiro/RJ - CEP 20030-021  
**Filial MG:** Av. Getúlio Vargas, nº 887/Sala 401 - Funcionários - Belo Horizonte/MG - CEP 30112-020  
**Filial DF:** SCN Quadra 01, Bloco F/Salas 102 a 104, Ed América Office Tower - Brasília/DF CEP 70711-905  
**Filial SP:** Rua Surubim, nº 577/5o andar - Ed. Igarassu - Brooklin - São Paulo/SP CEP - 04571-050  
**Integrasy:** Rua Alberto de Oliveira Santos, nº 42/Sala 1802, Edifício Pasteur - Centro, Vitória - ES - CEP: 29.010-364

---

## Cotação - Solução de segurança de endpoints

5 mensagens

---

**Raimundo Jose Campos Junior** <rjcampos@trt13.jus.br>

5 de maio de 2021 12:00

Para: ari.tavares@itgx.com.br

Cc: SETIC - Contratos <setic-contratos@trt13.jus.br>, Rodrigo Cartaxo Marques Duarte <rcduarte@trt13.jus.br>

Bom dia, Ari

Solicito cotação para projeto de segurança para endpoints, conforme especificações e quantitativos em anexo.

Att.

--

Raimundo José Campos Jr.

-----  
Técnico Judiciário - Apoio Especializado: Tecnologia da Informação  
Núcleo de Governança e Gestão de TIC - Escritório de Orçamento e Contratos de TIC  
Secretaria de Tecnologia da Informação e Comunicação  
Tribunal Regional do Trabalho da 13ª Região  
(83) 3533-6055



**Especificação antivirus.pdf**

139K

---

**Marta Coelho** <marta.coelho@itgx.com.br>

10 de maio de 2021 11:02

Para: rjcampos@trt13.jus.br

Bom dia Raimundo, tudo bem ?

Por gentileza poderia me passar razão social e CNPJ ?

Grata,

**Marta Coelho**

**ITGX TECNOLOGIA LTDA**

RJ : +55 (21) 2184-6609

SP : +55 (11) 3230-2273

Cel: +55 (21) 99175-9001

[www.itgx.com.br](http://www.itgx.com.br)

[Texto das mensagens anteriores oculto]

---

**Raimundo Jose Campos Junior** <rjcampos@trt13.jus.br>

10 de maio de 2021 13:25

Para: Marta Coelho <marta.coelho@itgx.com.br>

Boa tarde, Marta

Razão Social: Tribunal Regional do Trabalho da 13ª Região  
CNPJ: 02.658.544/0001-70

Att.

[Texto das mensagens anteriores oculto]

---

**Raimundo Jose Campos Junior** <rjcampos@trt13.jus.br>

11 de maio de 2021 13:42

Para: Marta Coelho <marta.coelho@itgx.com.br>

Cc: SETIC - Contratos <setic-contratos@trt13.jus.br>, Rodrigo Cartaxo Marques Duarte <rcduarte@trt13.jus.br>

Boa tarde, Marta

Solicito que a proposta seja encaminhada até sexta-feira com os quantitativos atualizados abaixo:

Item 1 - 82.809

Item 2 - 5.139

Item 3 - 28

Item 4 - 189

A proposta deve conter validade, que deverá ser igual ou superior a 30 dias.

[Texto das mensagens anteriores oculto]

---

**Marta Coelho** <marta.coelho@itgx.com.br>

12 de maio de 2021 00:32

Para: Raimundo Jose Campos Junior <rjcampos@trt13.jus.br>

Cc: SETIC - Contratos <setic-contratos@trt13.jus.br>, Rodrigo Cartaxo Marques Duarte <rcduarte@trt13.jus.br>

Olá, Raimundo! Tudo bem ?

Pode deixar, até sexta estaremos enviando!

Grata,

**Marta Coelho**

**ITGX TECNOLOGIA LTDA**

RJ : +55 (21) 2184-6609

SP : +55 (11) 3230-2273

Cel: +55 (21) 99175-9001

[www.itgx.com.br](http://www.itgx.com.br)

[Texto das mensagens anteriores oculto]



Raimundo Jose Campos Junior &lt;rjcampos@trt13.jus.br&gt;

---

**Re: Contato**

13 mensagens

**Breno Moreno Luna** <bluna@trt13.jus.br>

19 de abril de 2021 10:31

Para: Mauro Vicente &lt;mauro.vicente@avast.com&gt;, Raimundo Jose Campos Junior &lt;rjcampos@trt13.jus.br&gt;

Cc: SETIC - Contratos &lt;setic-contratos@trt13.jus.br&gt;

Obrigado pelo retorno Mauro!

Raimundo, que nos lê em cópia, entrará em contato com você para verificarmos a possibilidade de envio de proposta para participação em licitação.

Atenciosamente,

---

**Breno Moreno Luna**

Chefe do Núcleo de Governança de TIC

SETIC - Secretaria de Tecnologia da Informação e Comunicação

TRT13 - Tribunal Regional do Trabalho da 13ª Região

+55 (83) 3533.6055

+55 (83) 9.9983.0022 (Whatsapp)

Em seg., 19 de abr. de 2021 às 09:35, Mauro Vicente &lt;mauro.vicente@avast.com&gt; escreveu:

Prezado Breno,

Como posso ajuda-lo?

Att.

Mauro

Mauro Vicente

Regional Sales Manager - LATAM

+5511981229364 | [mauro.vicente@avast.com](mailto:mauro.vicente@avast.com) | [www.avg.com/partner](http://www.avg.com/partner)

---

**Mauro Vicente** <mauro.vicente@avast.com>

19 de abril de 2021 11:42

Para: Breno Moreno Luna &lt;bluna@trt13.jus.br&gt;, Raimundo Jose Campos Junior &lt;rjcampos@trt13.jus.br&gt;

Cc: SETIC - Contratos &lt;setic-contratos@trt13.jus.br&gt;

Prezados,

Poderiam me passar seu cnpj para cadastro? Já possuem algum ativirus?

Fico no aguardo do restante das informações para encaminhar a um parceiro que enviara a cotação.

Att.

Mauro

**Mauro Vicente**

Regional Sales Manager - LATAM

+5511981229364 | mauro.vicente@avast.com | www.avg.com/partner



[Texto das mensagens anteriores oculto]

---

**Breno Moreno Luna** <bluna@trt13.jus.br> 19 de abril de 2021 12:10  
Para: Mauro Vicente <mauro.vicente@avast.com>  
Cc: Raimundo Jose Campos Junior <rjcampos@trt13.jus.br>, SETIC - Contratos <setic-contratos@trt13.jus.br>

Já possuímos o McAfee. Segue os dados do Tribunal:

Tribunal Regional do Trabalho 13ª Região - Paraíba  
Av. Corálio Soares de Oliveira, S/N, Centro  
João Pessoa/PB - (próximo à Praça da Independência)  
CEP: 58013-260 - CNPJ: 02.658.544/0001-70  
Fone: (83) 3533-6000

---

**Breno Moreno Luna**

Chefe do Núcleo de Governança de TIC

SETIC - Secretaria de Tecnologia da Informação e Comunicação

TRT13 - Tribunal Regional do Trabalho da 13ª Região

+55 (83) 3533.6055

+55 (83) 9.9983.0022 (Whatsapp)

[Texto das mensagens anteriores oculto]

---

**Mauro Vicente** <mauro.vicente@avast.com> 19 de abril de 2021 12:17  
Para: Breno Moreno Luna <bluna@trt13.jus.br>  
Cc: Raimundo Jose Campos Junior <rjcampos@trt13.jus.br>, SETIC - Contratos <setic-contratos@trt13.jus.br>

Breno, quantas licenças e por quanto tempo?

[Texto das mensagens anteriores oculto]

---

**Breno Moreno Luna** <bluna@trt13.jus.br> 19 de abril de 2021 12:20  
Para: Mauro Vicente <mauro.vicente@avast.com>  
Cc: Raimundo Jose Campos Junior <rjcampos@trt13.jus.br>, SETIC - Contratos <setic-contratos@trt13.jus.br>

Mauro,

Peço aguardar o contato de Raimundo com esses detalhes. Ele irá enviar a especificação técnica, quantidade, modelo de negócio, etc... Ele deve enviar para você agora no início da tarde.

---

**Breno Moreno Luna**

Chefe do Núcleo de Governança de TIC

SETIC - Secretaria de Tecnologia da Informação e Comunicação

TRT13 - Tribunal Regional do Trabalho da 13ª Região

+55 (83) 3533.6055

+55 (83) 9.9983.0022 (Whatsapp)

[Texto das mensagens anteriores oculto]

---

**Raimundo Jose Campos Junior** <rjcampos@trt13.jus.br> 19 de abril de 2021 13:51  
Para: Breno Moreno Luna <bluna@trt13.jus.br>  
Cc: Mauro Vicente <mauro.vicente@avast.com>, SETIC - Contratos <setic-contratos@trt13.jus.br>

Boa tarde, Mauro

Ainda estou validando as especificações, assim que concluir eu te envio.  
Sobre as demais informações, são conforme tabela abaixo:

BENS E SERVIÇOS DA SOLUÇÃO ESCOLHIDA			
Item	Descrição	Unidade	Qtd.
1	Licença de software de segurança para estações de trabalho (endpoints) e servidores + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por <b>48 meses</b> .	Nº de licenças	81.157
2	Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por <b>48 meses</b> .	Nº de licenças	5.029
3	Implantação e configuração da solução + Repasse de conhecimento hands-on	Serviço	28
4	Treinamento EAD de capacitação técnica para administração da solução.	Nº de alunos	185

[Texto das mensagens anteriores oculto]

--

Raimundo José Campos Jr.

-----  
Técnico Judiciário - Apoio Especializado: Tecnologia da Informação  
Núcleo de Governança e Gestão de TIC - Escritório de Orçamento e Contratos de TIC  
Secretaria de Tecnologia da Informação e Comunicação  
Tribunal Regional do Trabalho da 13ª Região  
(83) 3533-6055

**Mauro Vicente** <mauro.vicente@avast.com>

19 de abril de 2021 14:53

Para: Raimundo Jose Campos Junior <rjcampos@trt13.jus.br>, Breno Moreno Luna <bluna@trt13.jus.br>

Cc: SETIC - Contratos <setic-contratos@trt13.jus.br>

Raimundo,

Obrigado pelas informações até agora.

Fico no aguardo da documentação.

Anexo 2 pdfs de produtos que julgo interessantes para proteção e manutenção de uma rede desse porte e que também pertencem a Avast Business.

Att.

Mauro



**Mauro Vicente**

Regional Sales Manager - LATAM

+5511981229364 | mauro.vicente@avast.com | www.avg.com/partner



**From:** Raimundo Jose Campos Junior <rjcampos@trt13.jus.br>  
**Date:** Monday, 19 April 2021 13:52  
**To:** Breno Moreno Luna <bluna@trt13.jus.br>  
**Cc:** Mauro Vicente <mauro.vicente@avast.com>, SETIC - Contratos <setic-contratos@trt13.jus.br>  
**Subject:** Re: Contato

Boa tarde, Mauro

Ainda estou validando as especificações, assim que concluir eu te envio.

Sobre as demais informações, são conforme tabela abaixo:

BENS E SERVIÇOS DA SOLUÇÃO ESCOLHIDA			
Item	Descrição	Unidade	Qtd.
1	Licença de software de segurança para estações de trabalho (endpoints) e servidores + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por 48 meses.	Nº de licenças	81.157
2	Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por 48 meses.	Nº de licenças	5.029
3	Implantação e configuração da solução + Repasse de conhecimento hands-on	Serviço	28
4	Treinamento EAD de capacitação técnica para administração da solução.	Nº de alunos	185

[Texto das mensagens anteriores oculto]

## 2 anexos



**data\_sheet\_patch\_br (1).pdf**  
53K



**CCleaner-Cloud-for-Business-Datasheet.pdf**  
7267K

**Mauro Vicente** <mauro.vicente@avast.com>

26 de abril de 2021 12:11

Para: Raimundo Jose Campos Junior <rjcampos@trt13.jus.br>, Breno Moreno Luna <bluna@trt13.jus.br>

Cc: SETIC - Contratos <setic-contratos@trt13.jus.br>

Prezados,

Obrigado pela informação até agora.

Gostaria de saber qual antivírus que vocês possuem.

De acordo com o complemento da informação faltante, poderei confirmar nosso pleno atendimento aos requisitos técnicos.

De antemão lhes asseguro uma proposta bem competitiva caso participemos.

Att.

Mauro

**Mauro Vicente**

Regional Sales Manager - LATAM

+5511981229364 | mauro.vicente@avast.com | www.avg.com/partner



**From:** Raimundo Jose Campos Junior <rjcampos@trt13.jus.br>  
**Date:** Monday, 19 April 2021 13:52  
**To:** Breno Moreno Luna <bluna@trt13.jus.br>  
**Cc:** Mauro Vicente <mauro.vicente@avast.com>, SETIC - Contratos <setic-contratos@trt13.jus.br>  
**Subject:** Re: Contato

Boa tarde, Mauro

Ainda estou validando as especificações, assim que concluir eu te envio.

Sobre as demais informações, são conforme tabela abaixo:

BENS E SERVIÇOS DA SOLUÇÃO ESCOLHIDA			
Item	Descrição	Unidade	Qtd.
1	Licença de software de segurança para estações de trabalho (endpoints) e servidores + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por 48 meses.	Nº de licenças	81.157
2	Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por 48 meses.	Nº de licenças	5.029
3	Implantação e configuração da solução + Repasse de conhecimento hands-on	Serviço	28
4	Treinamento EAD de capacitação técnica para administração da solução.	Nº de alunos	185

[Texto das mensagens anteriores oculto]

**Raimundo Jose Campos Junior** <rjcampos@trt13.jus.br>

6 de maio de 2021 18:04

Para: Mauro Vicente &lt;mauro.vicente@avast.com&gt;

Cc: Breno Moreno Luna &lt;bluna@trt13.jus.br&gt;, SETIC - Contratos &lt;setic-contratos@trt13.jus.br&gt;, Rodrigo Cartaxo Marques Duarte &lt;rcduarte@trt13.jus.br&gt;


Boa tarde, Mauro

Segue em anexo o documento com as especificações técnicas do projeto.

Att.

[Texto das mensagens anteriores oculto]

---

 **Especificação antivírus.pdf**  
139K

---

**Mauro Vicente** <mauro.vicente@avast.com>

7 de maio de 2021 10:21

Para: Raimundo Jose Campos Junior <rjcampos@trt13.jus.br>

Cc: Breno Moreno Luna <bluna@trt13.jus.br>, SETIC - Contratos <setic-contratos@trt13.jus.br>, Rodrigo Cartaxo Marques Duarte <rcduarte@trt13.jus.br>

Prezados,

Podemos conversar por telefone?

Gostaria de tirar uma dúvida com respeito ao projeto.

[Texto das mensagens anteriores oculto]

---

**Raimundo Jose Campos Junior** <rjcampos@trt13.jus.br>

7 de maio de 2021 17:22

Para: Mauro Vicente <mauro.vicente@avast.com>

Boa tarde, Mauro

Meu telefone é o (83) 9 9682 7470

[Texto das mensagens anteriores oculto]

---

**Mauro Vicente** <mauro.vicente@avast.com>

7 de maio de 2021 17:44

Para: Raimundo Jose Campos Junior <rjcampos@trt13.jus.br>

Raimundo,


Obrigado por seu tempo ao telefone.

O documento tem partes assinaladas em vermelho que não atendemos.

Caso queiram conhecer melhor nossa ferramenta, estamos à disposição.

[Texto das mensagens anteriores oculto]

---

 **Especificação antivírus[2].pdf**  
155K

---

**Raimundo Jose Campos Junior** <rjcampos@trt13.jus.br>

11 de maio de 2021 13:32

Para: Mauro Vicente <mauro.vicente@avast.com>

Boa tarde, Mauro

Conforme conversamos por telefone, infelizmente necessitamos desses requisitos que vossa solução não atende. Mas agradeço a presteza e a atenção dispensadas.

Att.

[Texto das mensagens anteriores oculto]

---

## Contato Mesquita TI

4 mensagens

**Pedro Mesquita** <pedro.mesquita@mtm-ti.com.br>

27 de abril de 2021 11:55

Para: "bluna@trt13.jus.br" <bluna@trt13.jus.br>

Cc: "Vicuna, Ruben" <Ruben.Vicuna@f-secure.com>, "setic-contratos@trt13.jus.br" <setic-contratos@trt13.jus.br>, "rjcampos@trt13.jus.br" <rjcampos@trt13.jus.br>

Bom dia,

Conforme falamos, segue meu contato.

Mesquita.



**PEDRO MESQUITA | Consultor**  
Skype: pedro.mesquita74  
pedro.mesquita@mtm-ti.com.br  
www.mtm-ti.com.br  
☎ 41 3408.2438    📞 41 9 9654.2439  
Rua Carmelina Cavassin 1280 · Barreirinha · CEP 82.220-170

**MTM**  
MESQUITA TI

Antivírus Corporativo  
AntiSpam  
**ADOTI**

---

**Breno Moreno Luna** <bluna@trt13.jus.br>

27 de abril de 2021 12:03

Para: Pedro Mesquita <pedro.mesquita@mtm-ti.com.br>

Cc: "Vicuna, Ruben" <Ruben.Vicuna@f-secure.com>, "setic-contratos@trt13.jus.br" <setic-contratos@trt13.jus.br>, "rjcampos@trt13.jus.br" <rjcampos@trt13.jus.br>

Pedro,

Conforme conversa por telefone, segue a última versão das especificações do processo de aquisição nacional do TRT13. Aguardamos sua análise e se possível, envio da proposta.

Atenciosamente,

---

**Breno Moreno Luna**

Chefe do Núcleo de Governança de TIC

SETIC - Secretaria de Tecnologia da Informação e Comunicação

TRT13 - Tribunal Regional do Trabalho da 13ª Região

+55 (83) 3533.6055

+55 (83) 9.9983.0022 (Whatsapp)

[Texto das mensagens anteriores oculto]



**Antivirus - Especificação Técnica e Quantidades.pdf**

136K

---

**Breno Moreno Luna** <bluna@trt13.jus.br>

27 de abril de 2021 12:17

Para: SETIC - Contratos <setic-contratos@trt13.jus.br>, Ruber van der Linden de Vierde <rvierde@trt13.jus.br>, Alessandra Mendes da Silva <asilva@trt13.jus.br>, Rodrigo Mafra <rmafra@trt13.jus.br>

Pessoal, análise da especificação feita pela FSecure. Não atende em grande parte.

Pedro, entrou em contato comigo por telefone.

---

**Breno Moreno Luna**

Chefe do Núcleo de Governança de TIC  
SETIC - Secretaria de Tecnologia da Informação e Comunicação  
TRT13 - Tribunal Regional do Trabalho da 13ª Região  
+55 (83) 3533.6055  
+55 (83) 9.9983.0022 (Whatsapp)

----- Forwarded message -----

De: **Pedro Mesquita** <[pedro.mesquita@mtm-ti.com.br](mailto:pedro.mesquita@mtm-ti.com.br)>  
Date: ter., 27 de abr. de 2021 às 12:07  
Subject: Re: Contato Mesquita TI  
To: Breno Moreno Luna <[bluna@trt13.jus.br](mailto:bluna@trt13.jus.br)>

Segue...

<p><b>PEDRO MESQUITA   Consultor</b> <b>Skype:</b> pedro.mesquita74 pedro.mesquita@mtm-ti.com.br www.mtm-ti.com.br ☎ 41 3408.2438    ☎ 41 9 9654.2439 Rua Carmelina Cavassin 1280 · Barreirinha · CEP 82.220-170</p>	 <p>MESQUITA TI</p>	<p>Antivírus Corporativo AntiSpam </p>
--	---	---

[Texto das mensagens anteriores oculto]

---

 **especificações TRT7 (2).doc**  
78K

---

**Pedro Mesquita** <[pedro.mesquita@mtm-ti.com.br](mailto:pedro.mesquita@mtm-ti.com.br)> 27 de abril de 2021 12:44  
Para: Breno Moreno Luna <[bluna@trt13.jus.br](mailto:bluna@trt13.jus.br)>  
Cc: "setic-contratos@trt13.jus.br" <[setic-contratos@trt13.jus.br](mailto:setic-contratos@trt13.jus.br)>, "rjcampos@trt13.jus.br" <[rjcampos@trt13.jus.br](mailto:rjcampos@trt13.jus.br)>, Cleverson Marqueti <[cleverson@securegate.com.br](mailto:cleverson@securegate.com.br)>, Caroline | SECURE GATE <[carol@securegate.com.br](mailto:carol@securegate.com.br)>

Boa tarde,

Conforme entendimento em nossa ligação, da forma ao qual está escritor o processo não conseguimos atender com F-Secure.

Copio o direto da distribuída, caso tenha algum entendimento, diferente do meu.

Mesquita.

**PEDRO MESQUITA | Consultor****Skype:** pedro.mesquita74

pedro.mesquita@mtm-ti.com.br

www.mtm-ti.com.br

☎ 41 3408.2438 ☎ 41 9 9654.2439

Rua Carmelina Cavassin 1280 · Barreirinha · CEP 82.220-170

**MTM**  
MESQUITA TI

Antivírus Corporativo

AntiSpam

**De:** Breno Moreno Luna <[bluna@trt13.jus.br](mailto:bluna@trt13.jus.br)>**Data:** terça-feira, 27 de abril de 2021 12:03**Para:** Pedro Mesquita <[pedro.mesquita@mtm-ti.com.br](mailto:pedro.mesquita@mtm-ti.com.br)>**Cc:** "[setic-contratos@trt13.jus.br](mailto:setic-contratos@trt13.jus.br)" <[setic-contratos@trt13.jus.br](mailto:setic-contratos@trt13.jus.br)>, "[rjcampos@trt13.jus.br](mailto:rjcampos@trt13.jus.br)" <[rjcampos@trt13.jus.br](mailto:rjcampos@trt13.jus.br)>**Assunto:** Re: Contato Mesquita TI

Pedro,

[Texto das mensagens anteriores oculto]

[Texto das mensagens anteriores oculto]

---

**[NIVA] Solução de Segurança de End-Point**

5 mensagens

---

**g.sousa@nivati.com.br** <g.sousa@nivati.com.br>  
Para: rjcampos@trt13.jus.br

4 de maio de 2021 10:55

Bom dia Raimundo,

O TRT13 está com esse processo de aquisição de solução de segurança de end-point em aberto?

Gostaríamos de participar e tomarmos ciências da documentação técnica.

Obrigado.



---

**Raimundo Jose Campos Junior** <rjcampos@trt13.jus.br>

6 de maio de 2021 18:00

Para: g.sousa@nivati.com.br

Cc: SETIC - Contratos &lt;setic-contratos@trt13.jus.br&gt;, Rodrigo Cartaxo Marques Duarte &lt;rcduarte@trt13.jus.br&gt;

Boa tarde, Gustavson

Estamos em fase de pesquisa de preço, após revisão e conclusão das especificações. Caso vocês atendam ao requisitado, gostaríamos de solicitar uma cotação.

Segue documento em anexo.

Att.


[Texto das mensagens anteriores oculto]

--

Raimundo José Campos Jr.

-----  
Técnico Judiciário - Apoio Especializado: Tecnologia da Informação  
Núcleo de Governança e Gestão de TIC - Escritório de Orçamento e Contratos de TIC  
Secretaria de Tecnologia da Informação e Comunicação  
Tribunal Regional do Trabalho da 13ª Região  
(83) 3533-6055

---

 **Especificação antivírus.pdf**  
139K

---

**Raimundo Jose Campos Junior** <rjcampos@trt13.jus.br>

11 de maio de 2021 13:44

Para: g.sousa@nivati.com.br

Cc: SETIC - Contratos <setic-contratos@trt13.jus.br>, Rodrigo Cartaxo Marques Duarte <rcduarte@trt13.jus.br>

Boa tarde, Gustavson

Solicito que a proposta seja encaminhada até sexta-feira com os quantitativos atualizados abaixo:

Item 1 - 82.809

Item 2 - 5.139

Item 3 - 28

Item 4 - 189

A proposta deve conter validade, que deverá ser igual ou superior a 30 dias.

[Texto das mensagens anteriores oculto]

---

**g.sousa@nivati.com.br** <g.sousa@nivati.com.br>

11 de maio de 2021 13:54

Para: Raimundo Jose Campos Junior <rjcampos@trt13.jus.br>

Cc: SETIC - Contratos <setic-contratos@trt13.jus.br>, Rodrigo Cartaxo Marques Duarte <rcduarte@trt13.jus.br>

Boa tarde estimado Raimundo,

Fizemos uma análise bastante minuciosa no processo, pois não tínhamos nenhuma visibilidade até então.

As 02 soluções que temos em nosso portfólio, Crowdstrike e Palo Alto, ambas são do tipo NGAV e não fazem parte de uma solução de antivírus tradicional. Por conta disto, os preços de solução do tipo NGAV são bastante superiores ao tradicional, inviabilizando a participação e até mesmo a vitória de um projeto tão vislumbrante com esse.

Não por isso, fico a inteira disposição para outros projetos no que tange a área de Segurança da Informação.

Obrigado.



[Texto das mensagens anteriores oculto]

---

**Raimundo Jose Campos Junior** <rjcampos@trt13.jus.br>

11 de maio de 2021 13:55

Para: g.sousa@nivati.com.br

Cc: SETIC - Contratos <setic-contratos@trt13.jus.br>, Rodrigo Cartaxo Marques Duarte <rcduarte@trt13.jus.br>

Sem problemas, agradeço a atenção.

Att.

[Texto das mensagens anteriores oculto]